TITOLO DOCUMENTO:	DigitalSign 3.1 – Manuale Utente

TIPO DOCUMENTO:	Manuale Utente
EMESSO DA:	IT Telecom s.r.l.
DATA EMISSIONE:	30/09/2010
N. ALLEGATI:	0
STATO:	Rilasciato

REDATTO:	A. Carlucci	ITT
VERIFICATO:	M. Donatone	ITT
APPROVATO:	M. Donatone	ITT
LISTA DI DISTRIBUZIONE:	ITT, Telecom Italia, Clienti Telecom Italia	TI

REGISTRO DELLE MODIFICHE		
REVISIONE	DESCRIZIONE	EMISSIONE
0	Prima Redazione (DigitalSign v3.1.3.1, documentazione v3.1.8)	30/09/2010

Sommario

Sommario

1 Dalla versione 3.0 alla versione 3.1

Questa edizione della Guida Utente di ***DigitalSign*** è aggiornata alla versione BETA 3.1.3.0.
La versione 3.1, rispetto alla 3.0, contiene alcune novità implementate per supportare le novità imposte dalla Deliberazione CNIPA 45/2009 e destinate ad entrare in vigore il 1 Settembre 2010, con possibilità di una introduzione anticipata fino a 90 giorni.

Le novità implementate sono qui riassunte:

- **Funzione Hash (art. 4, comma 1 e 2, art. 5)**
  Viene dismessa la funzione hash SHA-1, in favore di SHA-256
  Nessun documento informatico dovrebbe essere messo in circolazione dopo il 01/09/2010 recante una firma digitale basata su SHA-1.
  Naturalmente i documenti firmati prima di tale data con SHA-1 manterranno la propria validità.
  Non è materialmente possibile stabilire con certezza la data di sottoscrizione di un documento privo di marca temporale (il signing-time è una dichiarazione del sottoscrittore, non ha valore di prova): per questa ragione, dopo il 01/09/2010, presentando un documento firmato con SHA-1, DigitalSign emetterà un apposito messaggio di warning.
  Tutti i documenti firmati con una DigitalSign 3.1 impiegano la funzione hash SHA-256.
  Tutti i certificati e le CRL emesse da DigitalSign 3.1 sono firmati con la funzione SHA-256
- **Formato CAdES-BES (art.21, comma 1)**
  Il formato PKCS#7 si arricchisce secondo la specifica CAdES. In particolare si introduce un nuovo attributo “signed” (id-aa-signingCertificateV2) che consente di coprire con la firma anche il certificato usato per firmare.
  Analogamente a quanto esposto sulla funziona SHA-256, tutti i documenti firmati dopo il 01/09/2010 dovranno avere questo attributo, dopo tale data DigitalSign preseterà un warinig verificando documenti non marcati temporalmente in precedenza e privi di questo attributo.
- **Marche temporali (art. 17)**
  Qui si riflette la maggior parte delle novità operative.
  Innanzitutto si introduce la possibilità di associare una marca temporale ad una firma o una controfirma, secondo il formato CAdES-T. La marca temporale, quindi, non è più necessariamente un oggetto esterno al documento firmato, poi associato con metodi proprietari: la marca temporale entra strutturalmente nella busta crittografica, nello stesso file .p7m.
  Inoltre è possibile avere marche temporali distinte nel caso il documento contenga firme multiple.
  La complicazione consiste nel fatto che in generale, non essendo certo a priori che il documento contenga una sola firma, occorre navigare l’albero delle firme per localizzare quella che si intende corredare di marca temporale.
  È poi prevista un’altra modalità, più simile a quella usata in passato (file .p7x e .m7m), ma finalmente basata su uno standard (RFC 5544). I file prodotti hanno ora estensione .tsd.
  È difficile prevedere oggi quale di queste modalità si imporrà come “standard” operativo nei processi, o se entrambe coesisteranno per applicarsi a contesti leggermente diversi. In ogni caso le procedure esistenti, non fosse altro che per la differente *naming convention* dei file, dovranno essere riviste.
  Si noti che non è vietato continuare ad usare i formati .p7x e .m7m in luogo del nuovo .tsd; anzi, i formati sono compatibili, nel senso che è possibile convertire da uno all’altro formato. DigitalSign, almeno per ora, mantiene la possibilità di salvare i documenti in tutti i vecchi formati.

2 Generalità e Concetti

2.1 Principi e riferimenti normativi sulle firme elettroniche

2.1.1 Concetti di "firma elettronica" e "firma elettronica avanzata"

Una definizione di **firma elettronica**, tratta dalla Direttiva Comunitaria 1999/93/CE e ripresa dal nostro Codice dell'Amministrazione Digitale, è la seguente:

"un insieme di dati in forma elettronica, allegati o logicamente associati con altri dati elettronici e che servono come metodo di autenticazione".

Si tratta evidentemente di una definizione assai generale, in cui ricade un vasto spettro di strumenti. Anche scrivere il proprio nome in calce ad un messaggio email può essere considerato una forma di firma elettronica.
Naturalmente è più interessante considerare meccanismi che permettano di emulare (possibilmente superare) il funzionamento di una firma autografa apposta su un documento cartaceo.
La stessa Direttiva contiene una definizione di **firma elettronica avanzata**:

"una f.e. che soddisfa i seguenti requisiti:

1. *è univocamente collegata al sottoscrittore*
2. *permette di identificare il sottoscrittore*
3. *è collegata ai dati cui si riferisce in modo tale da rivelare qualsiasi modifica successiva a tali dati"*

Si noti che queste definizioni sono volutamente generali e che non entrano nel merito degli strumenti tecnologici utilizzabili per raggiungere gli obiettivi di firmare elettronicamente dei dati. Lo scopo di questa generalità, in un documento giuridico, è proprio quello di non condizionare il progresso tecnologico, lasciando liberi il mercato e l'industria di far emergere le soluzioni via via più efficaci e convenienti per implementare i principi qui enunciati.

2.1.2 La firma digitale

Volendo riprendere le definizioni del Codice dell'Amministrazione Digitale troviamo che:

- la **firma elettronica qualificata** è
  "la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un ***certificato qualificato*** *e realizzata mediante un* ***dispositivo sicuro per la creazione della firma****, quale l'apparato strumentale usato per la creazione della firma elettronica"*
- la **firma digitale** è
  "un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare provenienza e integrità di un documento informatico"

In altre parole, con “firma digitale” si intende di regola un particolare tipo di “firma elettronica avanzata”, realizzata mediante l’uso di algoritmi di *hashing* per derivare un’impronta dai dati oggetto della firma, e da algoritmi di crittografia asimmetrica per derivare la firma dall’impronta.

Le due chiavi di una coppia vengono gestite in modo che la chiave privata resti in totale ed esclusiva disponibilità del sottoscrittore, e che la chiave pubblica sia effettivamente accessibile a chiunque si trovi nella necessità di verificare una firma.
Per rendere la chiave pubblica effettivamente fruibile e per associare la coppia di chiavi ad una identità, si adotta lo strumento del certificato di chiave pubblica (si veda la prossima sezione).

Questa tecnica soddisfa i requisiti delle firme elettroniche perché:

1. la firma è generata con la chiave privata in possesso esclusivo del sottoscrittore, quindi è univocamente collegata a tale soggetto;
2. permette di identificare il sottoscrittore, perché un ente attendibile (certificatore) emette un certificato che associa la chiave pubblica ad una identità;
3. rivela ogni modifica successiva apportata ai dati, perché in fase di verifica non si avrebbe corrispondenza tra l’impronta calcolata sui dati e quella decifrata dalla firma.

Nel contesto giuridico italiano, a queste caratteristiche “tecniche” della firma digitale si aggiungono le restrizioni relative all’uso di un dispositivo sicuro per la conservazione delle chiavi private e di un certificato qualificato per attestare l’identità del sottoscrittore.

2.1.3 Il certificato di chiave pubblica

Elemento fondamentale di una cosiddetta “infrastruttura di chiave pubblica” è il **certificato**, che corrisponde direttamente ad una coppia di chiavi (privata e pubblica) associate ad un titolare.

Si tratta di un insieme di dati (possiamo pensare ad uno speciale documento o ad un file) contenente alcune informazioni fondamentali:

- numero di serie
- dati anagrafici o identificativi del titolare del certificato stesso
- copia della chiave pubblica della coppia associata al titolare
- data di emissione e data di scadenza del certificato
- indicazione del soggetto che ha emesso il certificato (Certificatore)
- informazioni ausiliarie per definire formato e caratteristiche di utilizzabilità del certificato
- indicazioni che consentono di verificare, tramite un accesso automatico al sistema del certificatore, l’eventuale stato di revoca anticipata della validità del certificato
- firma digitale, calcolata sul contenuto del certificato stesso, generata dal “Certificatore”

Il motivo per cui un certificato venga sempre generato con una vita a termine, quindi con una data di scadenza predefinita, è collegato alla necessità di non mantenere indefinitamente in uso una coppia di chiavi.
Infatti la chiave privata e la pubblica di una coppia sono legate da una relazione matematica. Anche se non è possibile calcolare direttamente la chiave privata essendo nota la pubblica, è possibile usare la cosiddetta "forza bruta" e provare tutte le combinazione sino a trovare la chiave giusta.
La contromisura è usare chiavi di tale lunghezza che un tale procedimento costi un tempo di elaborazione molto lungo, misurabile in anni, anche usando i più veloci supercomputer esistenti ai giorni nostri. E quindi postulare una durata massima di una coppia di chiavi – registrata nel certificato – molto minore di questo tempo minimo necessario per trovare una chiave privata.

Da notare che la firma digitale apposta dal Certificatore, coprendo tutti gli altri dati contenuti nel certificato stesso, ne protegge l'integrità – per il fatto che eventuali alterazioni verrebbero rivelate, per definizione, in fase di verifica di questa firma – e l'autenticità – perché la firma del certificatore garantisce, sotto la responsabilità di quest'ultimo e nei limiti preventivamente concordati, della veridicità dei dati contenuti –.

2.1.4 Il Certificatore

Sul piano tecnico il soggetto che emette certificati di chiave pubblica si definisce "Autorità di Certificazione" o "*Certification Authority*" o CA.

Una CA è un organo che genera i certificati con il contenuto predefinito e li firma digitalmente con una propria chiave privata (detta "chiave privata di certificazione").
Naturalmente, come qualunque altro soggetto che emette firme ed è quindi dotato di una chiave privata, la CA deve anche essere dotato di un certificato associato alla relativa coppia di chiavi. Tale certificato si chiama "Certificato di CA".

La domanda scontata è: "ma chi emette allora il certificato della CA? Chi lo firma?"
La risposta è, in generale: "una CA di livello superiore"

Evidentemente questa iterazione di livelli non può ripetersi all'infinito e, prima o poi, la "catena di certificazione" deve arrivare ad una fine.
Il certificato della CA di livello più alto non viene dunque emesso da alcun organo superiore, ma è emesso dalla stessa CA: si tratta di un certificato *"self-signed"* o "di tipo *root*".
La particolarità è che questi certificati sono firmati con la chiave privata appartenente alla stessa coppia la cui chiave pubblica è contenuta nel certificato.

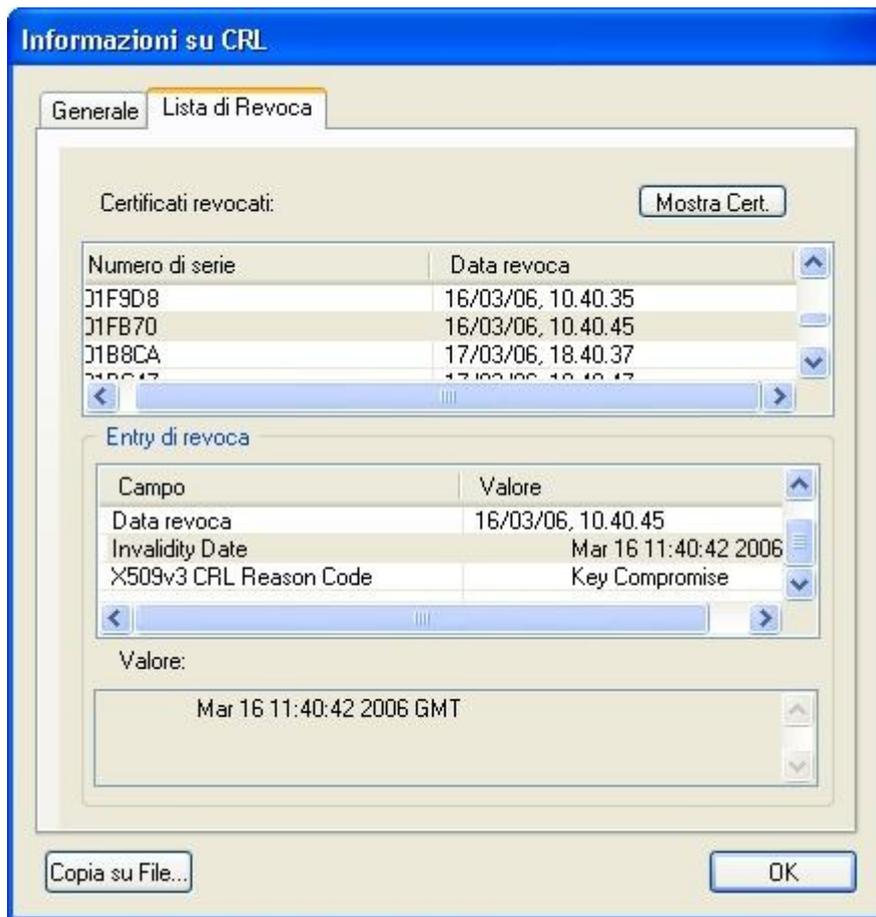
Tornando a livello di definizioni, la **CA** è normalmente intesa come l'organo tecnico, corrispondente ad una chiave privata ed un **certificato di CA**.
Il soggetto o ente che effettivamente svolge le attività correlate, viene definito "Certification Service Provider" o "Fornitore di Servizi di Certificatore", in breve "**Certificatore**".
Un Certificatore può, in generale, gestire più CA. Di solito questo avviene per emettere certificati di diversa tipologia (Firma Digitale, Autenticazione, Marcatura Temporale, ecc.).

2.1.5 Le liste di Sospensione e Revoca

Come spiegato nella sezione Il certificato di chiave pubblica un certificato nasce con una durata massima prefissata, dipendente dalla scelta commerciale del Certificatore che lo emette, ma comunque determinata dalla lunghezza delle chiavi oggetto di certificazione.

Tuttavia possono verificarsi diverse ragioni per terminare anzitempo la durata di un certificato. Il caso più tipico è quello del legittimo titolare ha perduto – o teme di aver perduto – il possesso esclusivo della chiave privata e vuole evitare che un malintenzionato emetta firme digitali a suo nome. Come si vede si tratta di un'esigenza molto simile al "blocco" di una carta di credito smarrita o rubata.

Ma la revoca di un certificato ha senso soltanto se chi verifica un documento firmato può determinare se il certificato associato alla firma è stato effettivamente revocato.
Lo strumento più comune (e l'unico attualmente fornito obbligatoriamente dai Certificatori) per soddisfa questa esigenza è la Lista di Sospensione e Revoca, o Certificate Revocation List (CRL).

Una CRL, banalmente, è una lista di numeri di serie di certificati emessi da una data CA, associati a data, ora e motivo della revoca.

La lista stessa è corredata da un’indicazione di data ed ora di emissione, nonché data ed ora della prossima emissione programmata. La lista è ovviamente firmata digitalmente dalla stessa CA e resa accessibile su un server, ad un indirizzo ben determinato.

Ogni certificato contiene l’indicazione dell’indirizzo Internet a cui è reperibile una copia della CRL. Poiché sia il certificato che la CRL sono firmate digitalmente dalla CA, l’integrità del sistema è molto protetta.
Naturalmente l’uso di queste liste dovrebbe essere automatico in fase di verifica di qualunque firma o certificato, rivelando se il certificato compare nella lista di revoca.

Il Certificatore dovrebbe aggiornare molto frequentemente le proprie CRL, in modo da rendere subito disponibili le revoche che possono avvenire in qualsiasi momento.

NOTA: le CRL si definiscono “Liste di Sospensione e Revoca” perché riportano sia lo stato di revoca che quello di sospensione. Senza entrare troppo nei dettagli possiamo dire che un certificato, di solito, viene posto in uno stato di sospensione (per esempio quando il titolare dichiara telefonicamente di aver perduto il possesso della chiave privata). In seguito, dopo una procedura amministrativa di controllo, la sospensione diventa una revoca a tutti gli effetti, oppure il certificato può sparire dalla lista (per esempio se il titolare dichiara poi di aver ritrovato una smartcard o se la segnalazione telefonica risulta poi non vera).

2.1.6 Il processo di verifica di una firma digitale

La meccanica della verifica di una firma consiste nella decifratura della firma stessa mediante la chiave pubblica dell'asserito sottoscrittore – ottenendo una copia dell'impronta – e nel confronto di tale valore con l'impronta calcolata direttamente sui dati, mediante l'appropriata funzione *hash*..

Tuttavia, al di là di verificare che il documento sia integro – operazione matematica priva di criticità – in un contesto reale è importante soprattutto verificare che il sottoscrittore sia veramente chi dice di essere e che il suo certificato sia in corso di validità.

Un documento firmato digitalmente contiene di norma (obbligatoriamente, nel caso dei documenti informatici a valore legale in Italia) una copia del certificato di ogni sottoscrittore.
Quindi il sistema di verifica ha a portata di mano la chiave pubblica per eseguire la verifica di integrità sopra descritta.

Ma per verificare l'identità del sottoscrittore il sistema deve verificare se il certificato è autentico.
A tale scopo si deve verificare la firma digitale della CA, apposta al certificato stesso.
Per verificare questa firma occorre disporre del certificato della CA; questo di regola è possibile conservando, a disposizione del proprio sistema, una lista dei certificati delle CA di proprio interesse.
Nel caso in cui il certificato della CA sia stato emesso da un'altra CA di livello superiore occorre risalire tutta la "catena di certificazione" fino al livello più alto (cioè fino a quando si trova il certificato *self-signed*, si veda Il Certificatore).
Giunti a questo punto, per essere sicuri che questo certificato sia autentico, occorre contare su una copia locale veramente attendibile. Se un malintenzionato è in grado di farci considerare attendibile un certificato *self-signed*, può anche costruire facilmente una falsa catena di certificazione e simulare qualunque identità.

In un vero contesto di gestione di documenti informatici questo è il punto più delicato: l'attendibilità dei certificati delle CA. Vedremo come DigitalSign implementa per questo fine accorgimenti ad elevato livello di sicurezza (non tutti i prodotti di firma digitale sul mercato possono dichiarare altrettanto), ma in questa sede ci limitiamo a portare il problema all'attenzione del lettore.

Dicevamo che oltre all'autenticità del certificato (ossia che sia stato veramente emesso da una CA considerata attendibile) occorre anche verificare che il certificato stesso sia in corso di validità.
Una prima verifica, banale, viene eseguita confrontando la data odierna con le date di emissione e scadenza registrate nel certificato stesso.

Quindi occorre verificare se il numero di serie del certificato compaia nella lista di revoca aggiornata pubblicata dal certificatore. Allora il procedimento consiste nei seguenti passi:

1. estrazione, dal certificato, dell'indirizzo da cui scaricare la CRL (CRL Distribution Pount)
2. scaricamento della CRL da tale indirizzo
3. verifica della firma della CA apposta alla CRL
4. verifica che la data ed ora attuali ricadano nell'intervallo tra la data ed ora di emissione e la data ed ora di prossimo aggiornamento pianificato della CRL
5. ricerca del numero di serie del certificato da verificare nella lista contenuta nella CRL

Naturalmente se la lista contiene effettivamente il numero di serie del certificato che stiamo verificando si deve concludere che il certificato, in questo momento, non è valido. E quindi

nemmeno il documento che contiene una firma apposta mediante quel certificato, a meno che non sia possibile dimostrare che il documento era stato firmato in precedenza, anteriormente alla revoca.

A partire dal 3 Dicembre 2009 entrano in vigore alcune novità contenute nelle Regole Tecniche rappresentate nel DPCM del 30 Marzo 2009.

In particolare:

- i certificatori non hanno più la libertà di rimuovere dalle proprie liste di sospensione e revoca le informazioni relative a certificati di cui sia ormai scaduta anche la validità nominale.
  Questa facoltà, utile ai certificatori per contenere il "peso" delle CRL, rendeva quasi impossibile (salvo chiedere le relative informazioni al Certificatore) accertare se in una data passata, compresa nell'intervallo di validità nominale di un certificato, tale certificato fosse anche indenne da provvedimenti di sospensione o revoca. Per raggiungere tale obiettivo in autonomia sarebbe stato necessario archiviare preventivamente tutte le copie rilevanti delle vecchie CRL.
  Oggi è invece possibile accertare la validità di un certificato in qualunque istante del passato solo controllando l'ultima CRL emessa da una data CA (esclusi, purtroppo, i certificati scaduti prima del 3 dicembre 2009);
- i software di verifica di firme digitali ufficiali dei diversi Certificatori devono offrire una specifica funzione di "Verifica alla data": la possibilità per l'utente di introdurre una data di riferimento passata ed ottenere la visualizzazione dello stato di validità del documento alla data indicata, piuttosto che quella odierna

Naturalmente DigitalSign offre questa funzionalità, particolarmente preziosa quando si verifichino documenti corredati di Marca Temporale.

2.1.7 Le Marche Temporali (*Timestamp*)

Una marca temporale è un documento informatico molto particolare.
È firmato digitalmente da un soggetto definito "Fornitore di Servizi di Marcatura Temporale" (*Timestamp Provider*, TSP) e contiene l'informazione precisa della data ed ora di emissione, nonché il valore di un'impronta fornito dall'utente.

Un utente utilizza questo servizio quando desidera associare una data certa all'esistenza di un documento:

1. si calcola il valore dell'impronta (*hash*) del documento oggetto della marcatura temporale
2. si trasmette, via Internet, al server del TSP una richiesta contenente l'impronta calcolata
3. si riceve la marca temporale (*timestamp*) dal server del TSP
4. si associa la marca temporale al documento

Poiché la firma digitale contenuta nel *timestamp* è considerata attendibile (se ci si rivolge a TSP accreditati presso CNIPA ha pieno valore di prova), sarà possibile dimostrare l'esistenza di un documento, per esempio, in un istante di tempo in cui il certificato del firmatario era sicuramente valido (non scaduto, non revocato).

La procedura di associare ad un documento firmato digitalmente una marca temporale viene anche denominata **consolidamento del valore probatorio**.

Con le novità normative introdotte nel DPCM 30 marzo 2009 (si veda la sezione precedente), ossia la permanenza nelle CRL delle informazioni di sospensione e revoca di certificati anche ormai scaduti, diventa possibile determinare immediatamente la validità probatoria di un documento marcato temporalmente: ***DigitalSign*** apre i documenti marcati temporalmente visualizzando immediatamente la verifica alla data corrispondente alla marca temporale, sollevando l'utente dall'incrocio manuale delle stesse informazioni.

2.2 Elementi di sicurezza previsti dalle norme italiane ed europee per la firma elettronica a massimo valore legale

2.2.1 Certificati qualificati

La Direttiva Comunitaria 1999/93/CE descrive un quadro di riferimento per le firme elettroniche a livello europeo. In tale contesto si tracciano i requisiti fondamentali per costruire un'infrastruttura affidabile in cui sia possibile raggiungere un livello di sicurezza sufficiente per considerare le firme elettroniche equivalenti a quelle tradizionali.

Un requisito di grande importanza è quello di poter associare in modo certo una firma all'identità del sottoscrittore, che – come descritto in Il Certificato di chiave pubblica – è proprio lo scopo del Certificato.
Un **Certificato Qualificato** è un certificato che offre particolari garanzie in termini di attendibilità. In particolare è emesso (con la propria firma elettronica avanzata) da un Certificatore che dimostra di possedere i requisiti per emettere Certificati Qualificati, tra cui citiamo i più significativi:

- provvede ad una accurata e responsabile identificazione fisica del soggetto titolare del certificato;
- mantiene un elenco dei certificati e dei soggetti titolari;
- implementa affidabili e tempestive procedure e servizi per la revoca dei certificati, garantendo che sia determinabile in modo preciso la data ed ora di ogni revoca;
- fa uso di sistemi e procedure affidabili in termini di sicurezza, nonché in termini di attendibilità e confidenzialità dei dati;

2.2.2 Dispositivi di firma

Un altro elemento di sicurezza prescritto dalla normativa per le firme elettroniche di massimo valore probatorio è dato dall'uso di oggetti definiti SSCD – *Secure Signature Creation Devices*, ossia Dispositivi Sicuri per la Creazione delle Firme, comunemente chiamati "dispositivi di firma". Si tratta di dispositivi specializzati, non programmabili se non dal produttore, capaci di almeno conservare le chiavi private al loro interno in modo che sia tecnicamente impossibile esportarle e di consentire l'uso delle proprie funzioni soltanto al legittimo proprietario.

Poiché una chiave privata non può mai uscire dal dispositivo, evidentemente non può essere sottratta da un malintenzionato se non sottraendo l'intero dispositivo.
Ma il dispositivo può essere attivato soltanto dal suo titolare: questo risultato si ottiene facendo sì che l'utente debba fornire al dispositivo una password (di solito interamente numerica, detta PIN) per attivarlo; se viene fornito un PIN errato per un numero molto limitato di volte consecutive il dispositivo va in stato di blocco. Per sbloccarlo occorre usare un apposito codice di sblocco (detto PUK); se anche questo codice viene introdotto in maniera errata per più volte il dispositivo va in blocco definitivo, senza possibilità di recupero.

Questo accorgimento impedisce, di fatto, l'utilizzo di un dispositivo rubato, a meno che il ladro non si impadronisca anche del codice PIN per l'utilizzo.

Poiché la chiave privata non può in nessun caso uscire dal dispositivo e poiché la chiave privata è necessaria per calcolare una firma, ne consegue che il calcolo stesso della firma viene effettuato dal dispositivo: il computer "ospite" del dispositivo trasmetterà al dispositivo il valore dell'impronta e ne otterrà in ritorno la firma calcolata.

Il tipo più comune di dispositivo di firma è la smartcard: semplice, economica, portabile, per l'utilizzo richiede un apposito lettore collegato al computer.
Va detto che le smartcard non sono tutte uguali, anche se hanno la stessa apparenza e se usano lo stesso standard di comunicazione attraverso i contatti visibili: quelle utilizzabili come SSCD devono disporre di apposita certificazione di conformità ai livelli di sicurezza imposti dalle norme.
Hanno il limite della lentezza operativa: sono in grado di calcolare circa una firma digitale al secondo.

Un dispositivo analogo alla smartcard è il token USB: una specie di chiavetta che inserisce direttamente in una porta USB del computer, contiene di fatto lo stesso chip presente in una smartcard ed offrono prestazioni dello stesso livello.

Per le applicazioni che richiedono elevati flussi operativi si utilizzano dispositivi chiamati HSM: sono schede per la crittografia veloce, capaci – secondo i modelli – di centinaia o migliaia di firma al secondo. Hanno costi elevati e vengono impiegati per procedure di firma automatica, per esempio per l'emissione di migliaia di fatture in tempi ristretti, ma anche dagli stessi Certificatori per l'emissione di Certificati e Marche temporali.

2.2.3 Accreditamento

La normativa prevede che un Certificatore che intende erogare certificati qualificati possa *accreditarsi* come tale presso CNIPA, il Centro Nazionale per l'Informatica nella Pubblica Amministrazione, organo che gestisce l'evoluzione stessa delle norme e vigila sul rispetto dei vincoli imposti.
L'accreditamento implica una forma di controllo da parte di CNIPA sulle attività dei Certificatori; non è una procedura obbligatoria (lo era prima dell'entrata in vigore della Direttiva Comunitaria in materia), ma allo stato non esiste alcun Certificatore non accreditato che emetta certificati qualificati.

2.2.4 La firma digitale *forte* e l'Attestazione, o *Firma Debole*

In taluni contesti si desidera trarre vantaggio dalla tecnologia della firma digitale per attuare una forma di autenticazione dei documenti, ma senza la necessità di conferire agli stessi documenti il massimo valore probatorio fornito dalle norme.
Vale la pena richiamare il contenuto dei primi due commi del Codice dell'Amministrazione Digitale (D.L. 82/2005):

Art. 21.
Valore probatorio del documento informatico sottoscritto

1. Il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza.

2. Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che sia data prova contraria.

Onde evitare confusione va qui specificato che la firma digitale cui ci si riferisce nel comma 2, in base alle definizioni dello stesso Decreto Legislativo, è quella avanzata, che realizza tutti i vincoli descritti nelle sezioni precedenti e che, proprio per la sua qualità, ha la massima valenza probatoria.

Ma come si può notare anche il comma 1 lascia spazio al valore probatorio delle firme elettroniche meno sofisticate, lasciando al giudice il compito di valutarne l'effettiva efficacia probatoria in funzione delle *caratteristiche oggettive di qualità e sicurezza*.

Molte organizzazioni desiderano utilizzare i certificati di autenticazione forniti su smartcard (ad esempio le "Carte Cittadino" del progetto SISS – Regione Lombardia) per "firmare" documenti. Allo scopo di ridurre il rischio di confusione non useremo il termine ***"firma"*** in questo caso, bensì il termine ***"attestazione"***.

3 Installazione e registrazione

3.1 La procedura di installazione

L'installazione di DigitalSign è di per sé un processo piuttosto semplice.
Tuttavia va tenuto presente che il prodotto DigitalSign esiste in diverse edizioni, dai contenuti anche molto differenti tra un'edizione e l'altra.
Inoltre spesso DigitalSign viene distribuito da distributori, rivenditori, organizzazioni che lo integrano nei propri sistemi e provvedono a fornire un ambiente di installazione integrato, spesso congiuntamente a software specifico per particolari smartcard, lettori, ecc.; in tal caso occorre seguire le istruzioni pratiche del fornitore.

In generale L'installazione di DigitalSign vero e proprio consiste in un solo file eseguibile da lanciare per avviare il processo di installazione vero e proprio.

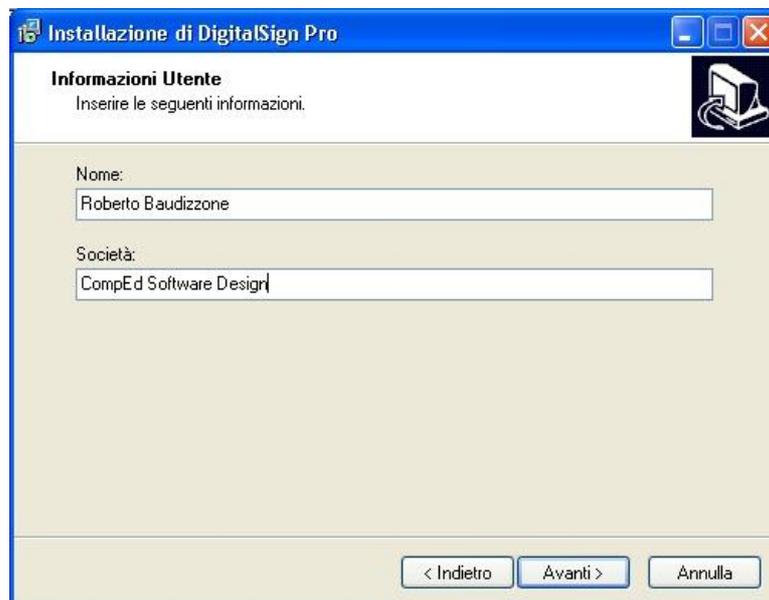
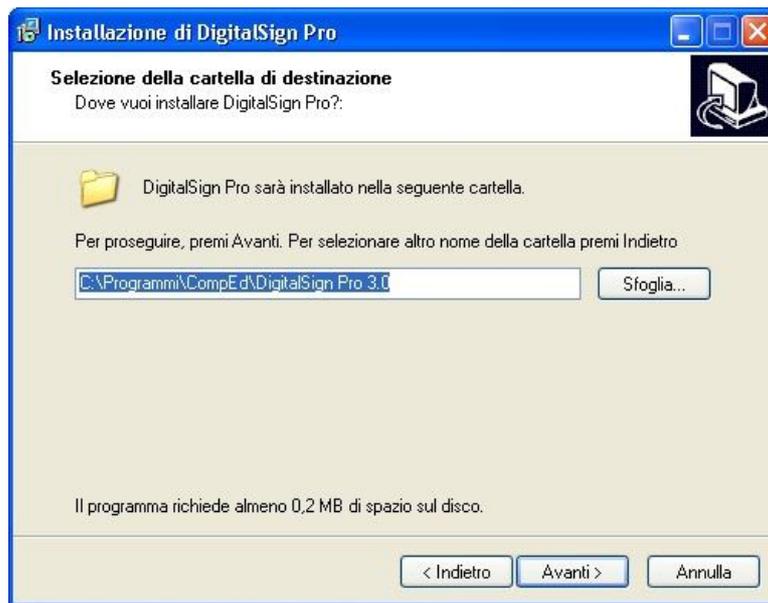
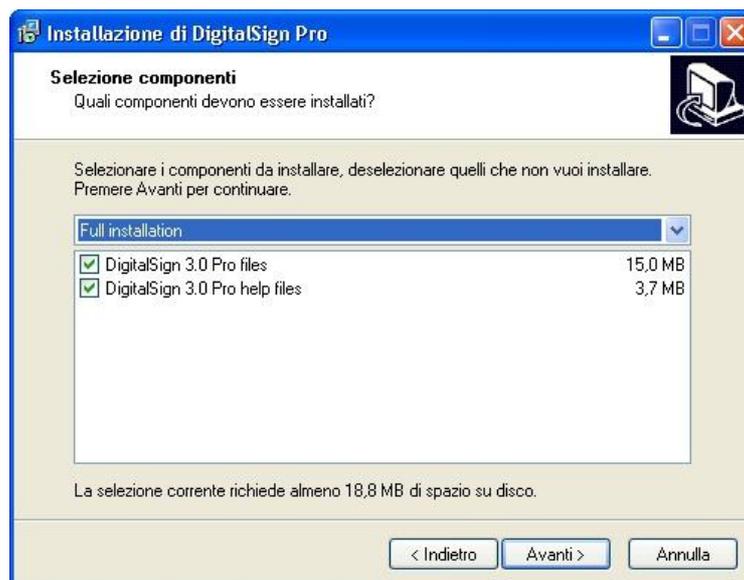
Ad esempio, scaricando DigitalSign Professional da un sito Internet si può ottenere il file

`DS31_PRO_R01.EXE`

Questo è il file di installazione per DigitalSign Professional 3.1.3.1.

Normalmente l'utente che vede questo file attraverso gli strumenti del proprio sistema farà doppio click su questo programma per avviare il processo di installazione.

Procedendo fase dopo fase, agendo sul bottone **Avanti**, si dovrà innanzitutto accettare le condizioni di licenza d'uso:

Quindi introdurre il proprio nominativo e quello dell'organizzazione di appartenenza, notando che questi dati non vengono trasmessi da DigitalSign, ma vengono solo registrati nel sistema.
È appena il caso di notare che prima di installare ed utilizzare una copia di DigitalSign occorre averne acquistato regolare licenza.

Sarà poi necessario confermare il percorso di installazione proposto dal programma, oppure indicarne uno alternativo; di norma è consigliabile accettare il percorso proposto, soprattutto per la facilità di trovare file e componenti nel caso si dovesse ricorrere al supporto tecnico;

Quindi dovremo scegliere altre opzioni di installazioni, in questo caso per avere o meno i file della documentazione:

L’utente può anche scegliere in quale cartella del menu avvio inserire i collegamenti per avviare DigitalSign; anche in questo caso è consigliabile accettare le impostazioni predefinite:

Al termine viene riproposta una scermata riassuntiva delle scelte fatte, con la richiesta di conferma o lìndicazione di tornare indietro ai passi precedenti per modificare una o più scelte:

A questo punto, dopo aver avviato il processo di installazione con il bottone **Installa**, la procedura inizia a posizionare i file mostrando una barra di progresso:

L'installazione termina con questa schermata (talvolta può essere richiesto di avviare il sistema):

Si rammenta ancora una volta che l'installazione di DigitalSign NON COMPRENDE l'installazione di software specifico per lettori e/o smartcard e che tale software deve essere installato separatamente.

3.1.1 L'installazione "silente"

Alcune edizioni di DigitalSign, soprattutto quelle distribuite da grandi organizzazioni, supportano una modalità di esecuzione silente: il processo di installazione viene eseguito con le impostazioni predefinite, senza richiedere l'intervento dell'operatore.

Nei casi in cui questa modalità è supportata può venire attivata a livello di linea comandi. Ad esempio, se il file di installazione è **`ds31_lisit_r01.exe`**, la linea comandi può essere:

- `ds31_lisit_r01 /silent`
  In questo caso il processo di installazione mostra soltanto la schermata con il progresso dell'installazione e null'altro, senza fermarsi a chiedere conferme o scelte dell'operatore.
- `ds31_lisit_r01 /verysilent`
  In questo caso il processo di installazione non mostra nulla e l'installazione avviene in modo invisibile per l'utente.

3.2 Registrazione ed Attivazione

Alcune edizioni di DigitalSign prevedono – in via opzionale od obbligatoria – l'esecuzione di una procedura di registrazione.

- **DigitalSign Professional CompEd** – la procedura di registrazione è facoltativa.
  Se la copia a disposizione viene registrata non viene più mostrato un banner informativo sui prodotti CompEd.
  La registrazione – comprensiva del Vendor ID – è obbligatoria per attivare le funzionalità COM e consentire l'utilizzo da parte di altre applicazioni.
- **DigitalSign Professional OEM** – di norma non è prevista alcuna registrazione, se non per attivare le funzionalità COM
- **DigitalSign Professional Integrated** – la procedura di registrazione è obbligatoria e richiede il Vendor ID
- **DigitalSign Lite** – la procedura di registrazione è obbligatoria e non è previsto il funzionamento dell'interfaccia COM, nemmeno fornendo il Vendor ID
- **DigitalSign Reader** – la procedura di registrazione è obbligatoria; occorre fornire anche un Vendor ID per attivare le funzionalità COM

Il processo di registrazione ed attivazione prevede tre momenti distinti:

1. raccolta informazioni di registrazione – l'utente è invitato ad inserire alcune informazioni, tra cui l'autorizzazione al trattamento, che vengono poi unite ad un "codice prodotto", calcolato automaticamente sulla base della particolare copia di DigitalSign a disposizione e sulla particolare macchina su cui è installata
2. trasmissione a CompEd – i dati raccolti, sempre chiaramente visibili, vengono trasmessi a CompEd che provvede ad elaborarle ed a generare un "codice di attivazione", che viene ritornato all'utente.
   Le informazioni possono essere trasmesse a CompEd mediante un collegamento diretto via Internet, oppure via email, o – in casi eccezionali – con mezzi diversi, per esempiop via fax.
3. trasmissione del "codice di attivazione all'utente" – il codice di attivazione viene impostato nel sistema, completando la procedura ed attivando il funzionamento previsto per la copia registrata.
   Salvo il caso di DigitalSign Professional Integrated le informazioni vengono sempre ritornate da CompEd all'utente via email.

Per le edizioni che prevedono la registrazione obbligatoria questa viene eseguita automaticamente al primo avvio. Per quelle che la prevedono in via opzionale compare una maschera di promemoria, oppure è possibile lanciarla dal menu Aiuto -> Procedura di Registrazione.

Il checkbox **Passa direttamente alla fase di attivazione** permette di saltare la fase di raccolta dati. Può essere utile per registrare nuovamente una copia del software quando già si dispone del codice di attivazione.
Il testo mostrato nella finestra contiene un link per visualizzare le informazioni relative alla modalità di trattamento, da parte di CompEd, dei dati che stanno per essere inviati.
Con il bottone **Avanti** si procede:

I campi del primo riquadro riguardano i dati personali di registrazione. Solo il campo **Nominativo** ed **Email** sono obbligatori, ma è obbligatorio anche selezionare il *checkbox* **Autorizzo CompEd…..**

Il secondo riquadro contiene un *checkbox* da selezionare se si dispone di un **Vendor ID**.

Il Vendor ID è un codice assegnato ai rivenditori di CompEd che dispongono di una licenza che li autorizza a sviluppare applicazioni intorno a DigitalSign; se il rivenditore desidera che il proprio cliente possa usare DigitalSign in modo integrato nei propri prodotti software dovrà far s^ che l'interfaccia COM di DigitalSign sia attiva e dovrà quindi fornire il proprio codice (Vendor ID) al cliente per l'installazione (oppure effettuare l'installazione/attivazione in prima persona).

Il terzo riquadro, Metodo di registrazione, permette di scegliere la modalità per recapitare i dati a CompEd:

- **Trasmetti on-line** – è il metodo preferito: DigitalSign si connette direttamente al server di CompEd e trasmette via web i dati di registrazione, così che il server possa immediatamente generare e ritrasmettere il codice di attivazione.
  Naturalmente questo metodo può essere usato solo se il computer ha un collegamento ad Internet privo di restrizioni per l'accesso alla rete.

  Come si vede la finestra visualizza il contenuto dei dati trasmessi e l'indirizzo di spedizione (quest'ultimo può essere utile per la diagnostica di eventuali problemi di rete; si noti che diverse versioni del software possono trasmettere a diversi indirizzi, quello riportato in figura ha solo valore indicativo).
  Con il bottone **Trasmetti** avviene il collegamento effettivo.

- Genera email – è un metodo simile al precedente, ma DigitalSign confeziona automaticamente un messaggio email pronto alla spedizione.

Da questa schermata si deve agire sul bottone Genera email per ottenere la costruzione automatica del messaggio.

A questo scopo viene utilizzato il client di posta MAPI predefinito: questo meccanismo non presenta controindicazioni con i software di email più diffuso (Miscrosoft Outlook ed Outlook Express), ma i risultati con altri prodotti dipendono dalla compatibilità di tali prodotti con le specifiche in questione.

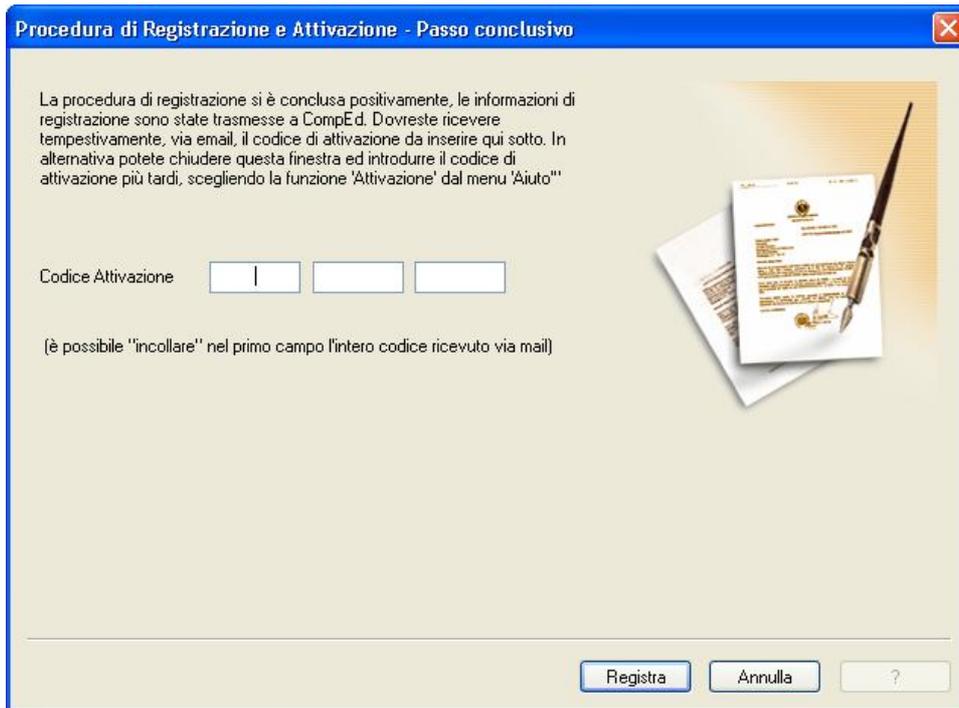
Ecco il risultato con Outlook:

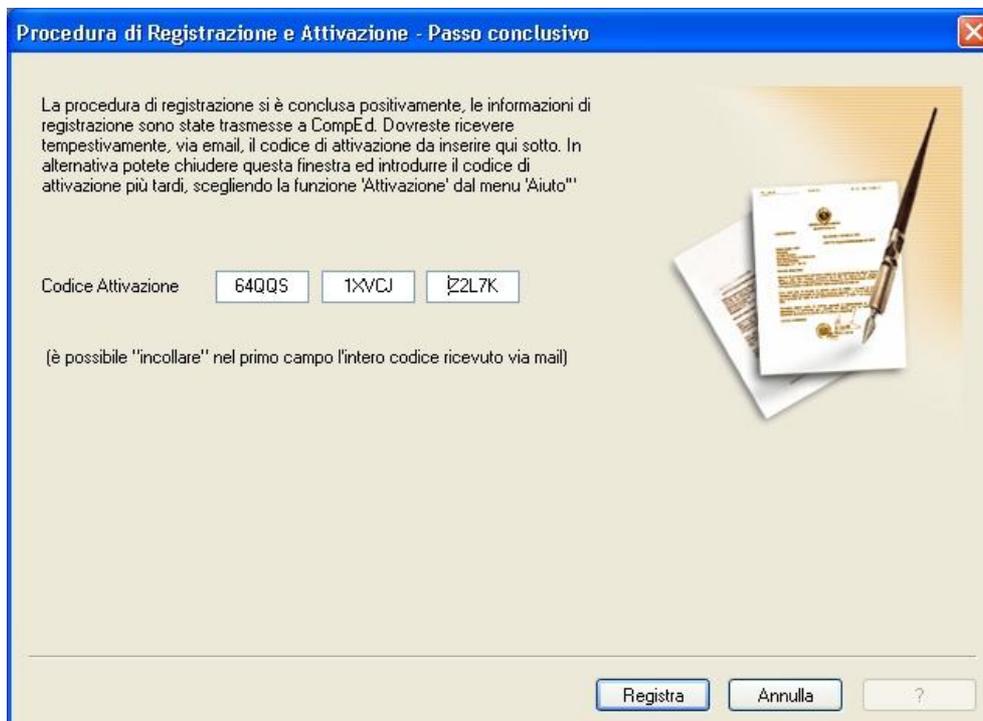
Il messaggio è facilmente ispezionabile prima dell'invio.
È di particolare importanza che il messaggio contenga l'allegato **`reg.txt`**, perché il server di registrazione elabora proprio tale allegato.
Qualora la macchina su cui si esegue la registrazione non avesse la possibilità di trasmettere email sarà comunque possibile copiare manualmente il file **`reg.txt`** su un altro computer e trasmetterlo, come allegato, all'indirizzo **registration@comped.it** .

- Genera fax – in casi eccezionali, ove non sia possibile trasmettere i dati di registrazione per web o per email, è possibile trasmettere a CompEd un fax con i dati di registrazione.

Con il bottone Genera fax si ottiene questa finestra:

Questa pagina può essere direttamente stampata e trasmessa per fax al numero indicato.
La procedura di registrazione via fax deve essere considerata solo una risorsa eccezionale, perché i tecnici di CompEd saranno costretti a trascriverli manualmente, con significativi rischi di errore.
Il codice di attivazione verrà comunque ritrasmesso via email.

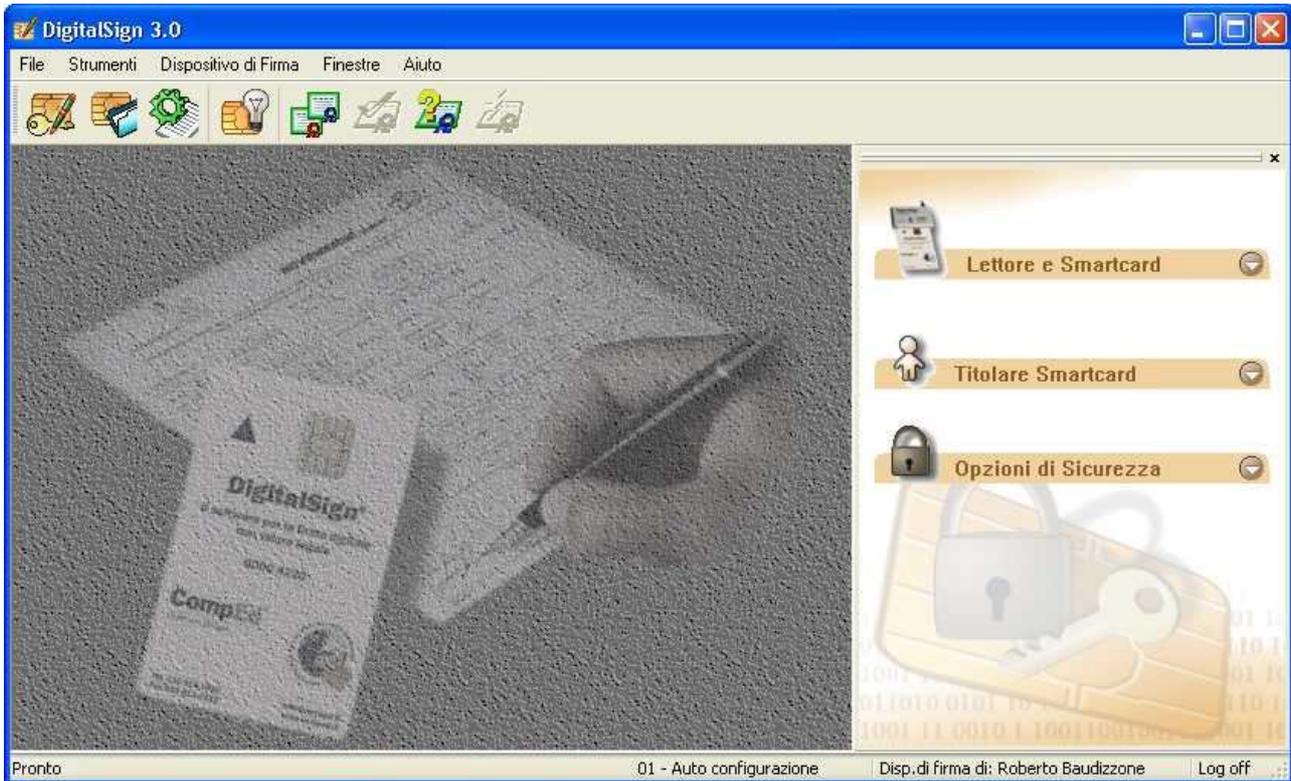
Indipendentemente dal metodo prescelto, con la successiva schermata DigitalSign si aspetta che l'utente introduca il codice di attivazione ottenuto da CompEd:

Nel frattempo il server di CompEd avrà trasmesso – all'indirizzo email indicato con la registrazione – un messaggio di questo tipo:

Il messaggio contiene il codice di attivazione. Sarà sufficiente selezionare il codice con il mouse e usare il comando “Copia” (Ctrl-C), quindi tornare alla finestra di DigitalSign ed “incollare (Ctrl-V) il codice nel primo campo:

Con il bottone Registra l’operazione è conclusa.

Si ricorda ancora che, nel caso l'intero ciclo non possa concludersi in soluzione unica, questa schermata può essere richiamata direttamente eseguendo la funzione del menu **Aiuto -> Attivazione** oppure la funzione di Registrazione sopra descritta selezionando il *checkbox* **Passa direttamente alla fase di attivazione**.

4 Riferimento

4.1 DigitalSign sullo schermo

4.1.1 La finestra principale

La finestra principale di DigitalSign presenta un menu di opzioni di base ed una vista sui pannelli informativi.

In realtà capita di rado di vedere la finestra principale priva di altre finestre, perché normalmente l'applicazione si apre direttamente mostrando una finestra documento.

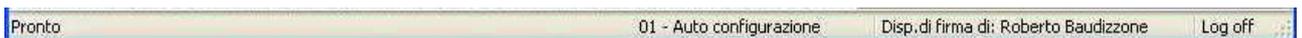
Da notare che la zona grigia della finestra principale è un'area *drag & drop*, ossia supporta il trascinamento degli oggetti. Questo significa che se da un'altra applicazione (tipicamente Explorer/Gestione Risorse) si trascina un documento in quest'area, il documento viene immediatamente aperto da DigitalSign.

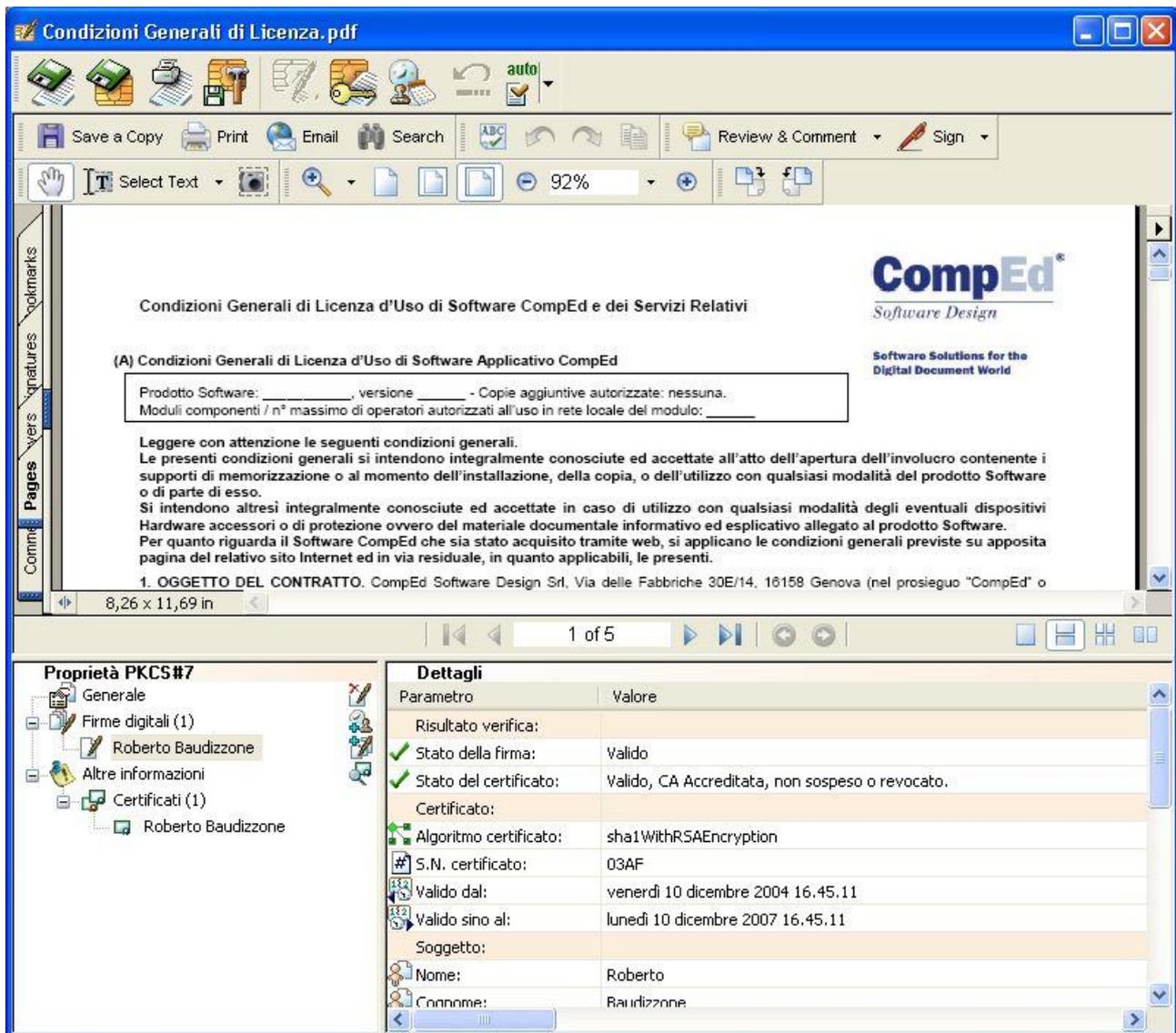
In ogni caso La finestra principale di DigitalSign presenta alcuni elementi fondamentali:

- Una barra menu

- Una barra strumenti

- Un’area di pannelli informativi

- Una barra di stato

4.1.2 La finestra documento

DigitalSign gestisce ogni documento all'interno di una di queste finestre, realizzando una vera e propria modalità **WYSIWYS** *(What You See Is What You Sign)*.

La finestra può contenere dettagli differenti in funzione della tipologia specifica del documento (in questo caso si tratta di un documento PDF e la visualizzazione avviene ad opera del software Adobe), ma il contesto è comune a tutti i casi.

Dall'immagine si evidenziano diversee aree:

- una **toolbar documento**, diversa da quella della finestra principale, ma che opera con lo stesso principio (ogni icona è associata ad una diversa funzione di menu);
- un'area **Viewer**, nella quale viene presentato all'utente il contenuto del documento su cui si sta operando;
- un'area **Proprietà PKCS#7**, nella quale sono presentati gli oggetti contenuti nella struttura del documento (firme, certificati, ecc.);
- un'area **Dettagli**, in cui sono visualizzate le informazioni di dettaglio riguardanti l'oggetto correntemente selezionato nell'area "Proprietà PKCS#7"

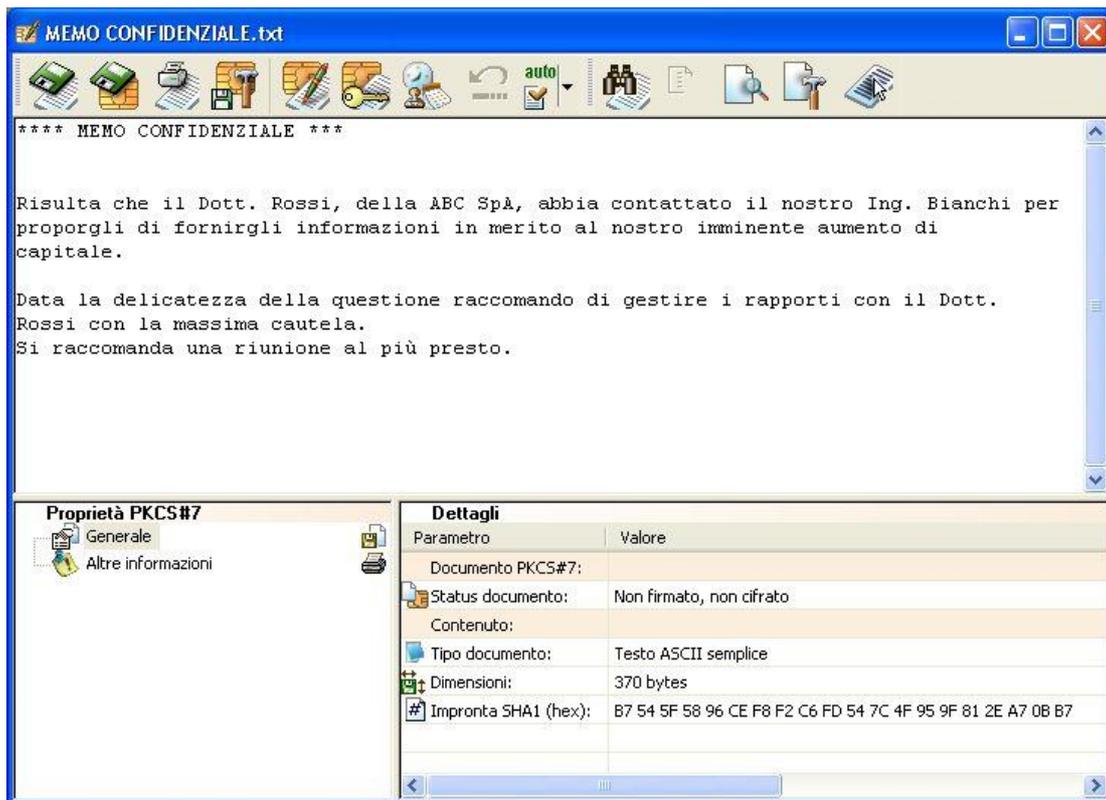
4.1.2.1 Finestra documento: area “Viewer”

Questa area di visualizzazione della finestra documento è fondamentale per la realizzazione della *modalità WYSIWYS (What You See Is What You Sign)*, perché qui è alloggiato lo specifico *viewer* di documento.
Un *viewer* è appunto un visualizzatore, ossia un componente software o un programma che si fa carico della visualizzazione del contenuto informativo del documento su cui si sta operando.

DigitalSign è effettivamente in grado di manipolare documenti elettronici di qualunque tipo e, per definizione, un documento elettronico può contenere dati binari che rappresentano informazioni intelligibili per mezzo di una certa applicazione.
Affinché DigitalSign possa provvedere alla presentazione dei dati di un documento deve utilizzare un viewer capace di interpretare correttamente i dati e, appunto, presentarli in modo coerente e significativo.

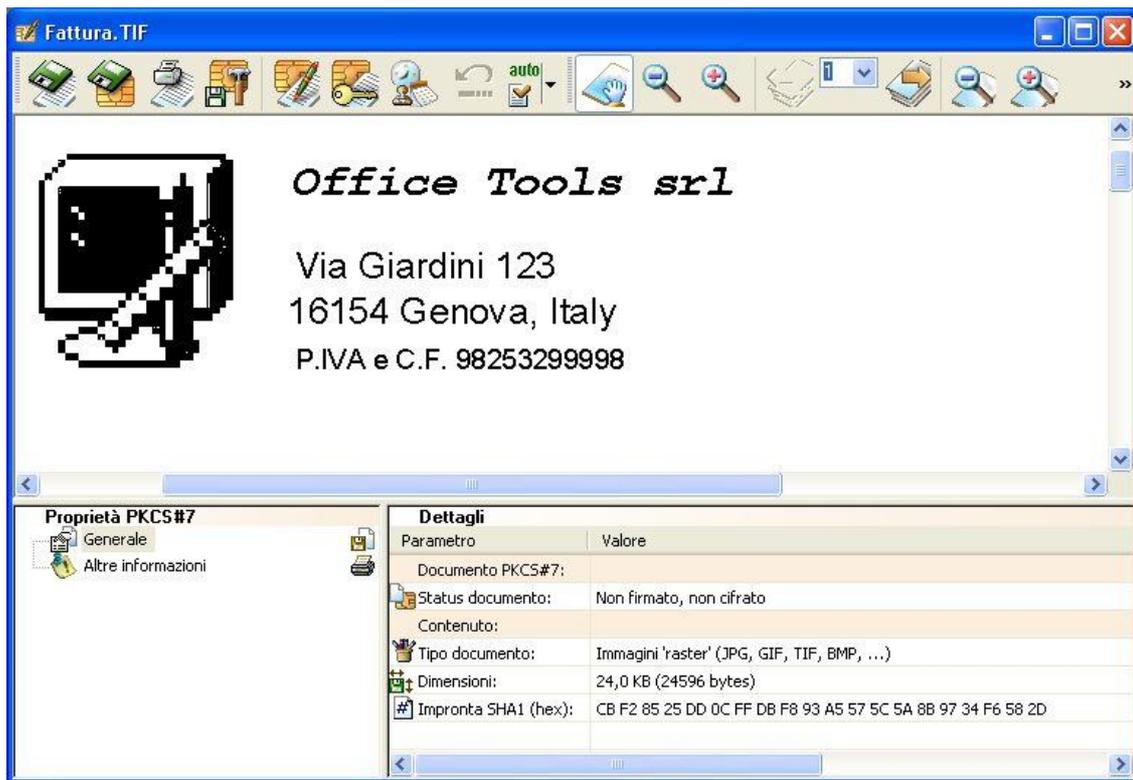
A questo punto è necessario distinguere tra diversi tipi di documento: come è noto il tipo viene convenzionalmente definito tramite una estensione (solitamente di 3 caratteri) che viene associata al nome del file che rappresenta il documento elettronico, separato dal carattere '.' (punto).

La visualizzazione dei diversi tipi di documento avviene dunque attraverso diversi tipi di *viewer*:

- ***SecurView ASCII: viewer per documenti di tipo testo***
  Questo viewer è totalmente integrato in DigitalSign. Questo significa che per la visualizzazione di questo tipo di documenti DigitalSign non fa ricorso ad alcuna applicazione esterna, né ad alcuna libreria di terze parti.
  Il documento viene mantenuto in un'area di memoria riservata di DigitalSign e da lì viene visualizzato.
  Quindi si tratta di un viewer ad elevato grado di sicurezza.

Il testo è interpretato secondo la codifica ASCII (standard).
I documenti elettronici di questo tipo hanno estensione **.TXT**
Lo standard ASCII riguarda caratteri espressi con 7 bit. Come è noto, tuttavia, i file gestiti da un PC contengono dati ad 8 bit; normalmente l'ottavo bit viene utilizzato per rappresentare le estensioni dell'ASCII a caratteri dipendenti dagli alfabeti nazionali e semigrafici. Tali estensioni dipendono dalla configurazione del PC e si dovrebbe tenerne conto valutando il contenuto di documenti contenenti caratteri di codice ASCII > 127.

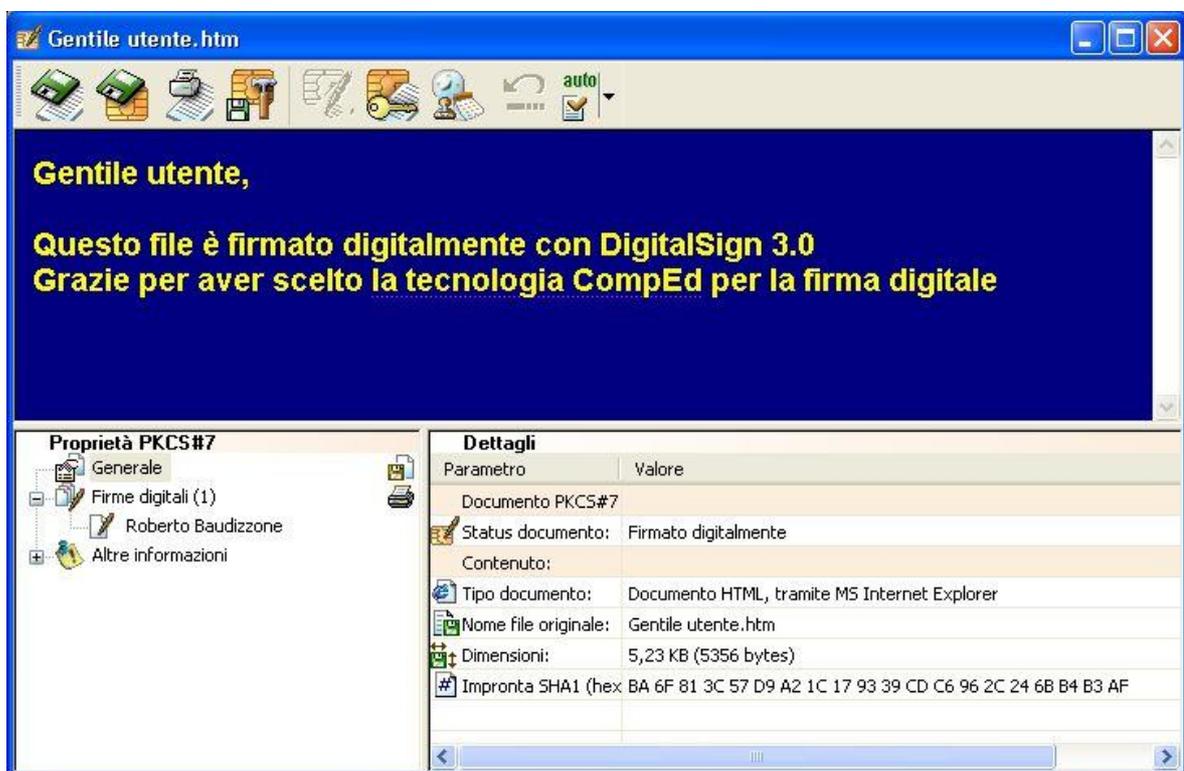
- ***SecurView RTF: viewer per documenti in Rich Text Format***
  Questo viewer è totalmente integrato in DigitalSign. Questo significa che per la visualizzazione di questo tipo di documenti DigitalSign non fa ricorso ad alcuna applicazione esterna, né ad alcuna libreria di terze parti, ma solo delle librerie di sistema Microsoft.
  Il documento viene mantenuto in un'area di memoria riservata di DigitalSign e da lì viene visualizzato.
  Quindi si tratta di un viewer ad elevato grado di sicurezza.

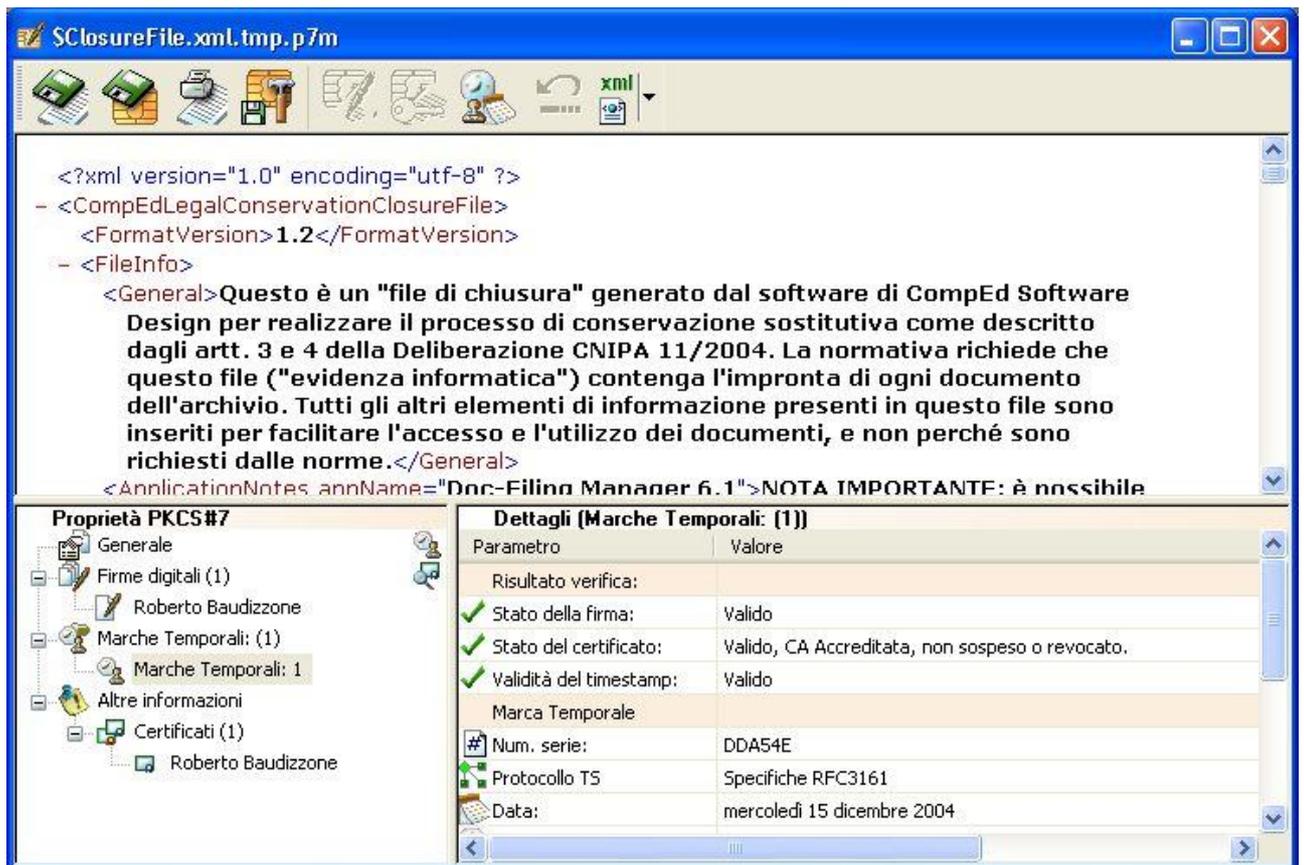
Il *Rich Text Format* è un formato che rappresenta informazioni testuali arricchite da diversi attributi per controllare, principalmente, la scelta del font, la dimensione del carattere, vari attributi grafici del testo.
L'interpretazione/presentazione di DigitalSign è basata sulle Microsoft Rich Text Format (RTF) Specifications, versione 1.5 (per riferimento si veda la Microsoft Development Network Library, Article ID: Q164472).
I documenti elettronici di questo tipo hanno estensione **.RTF**

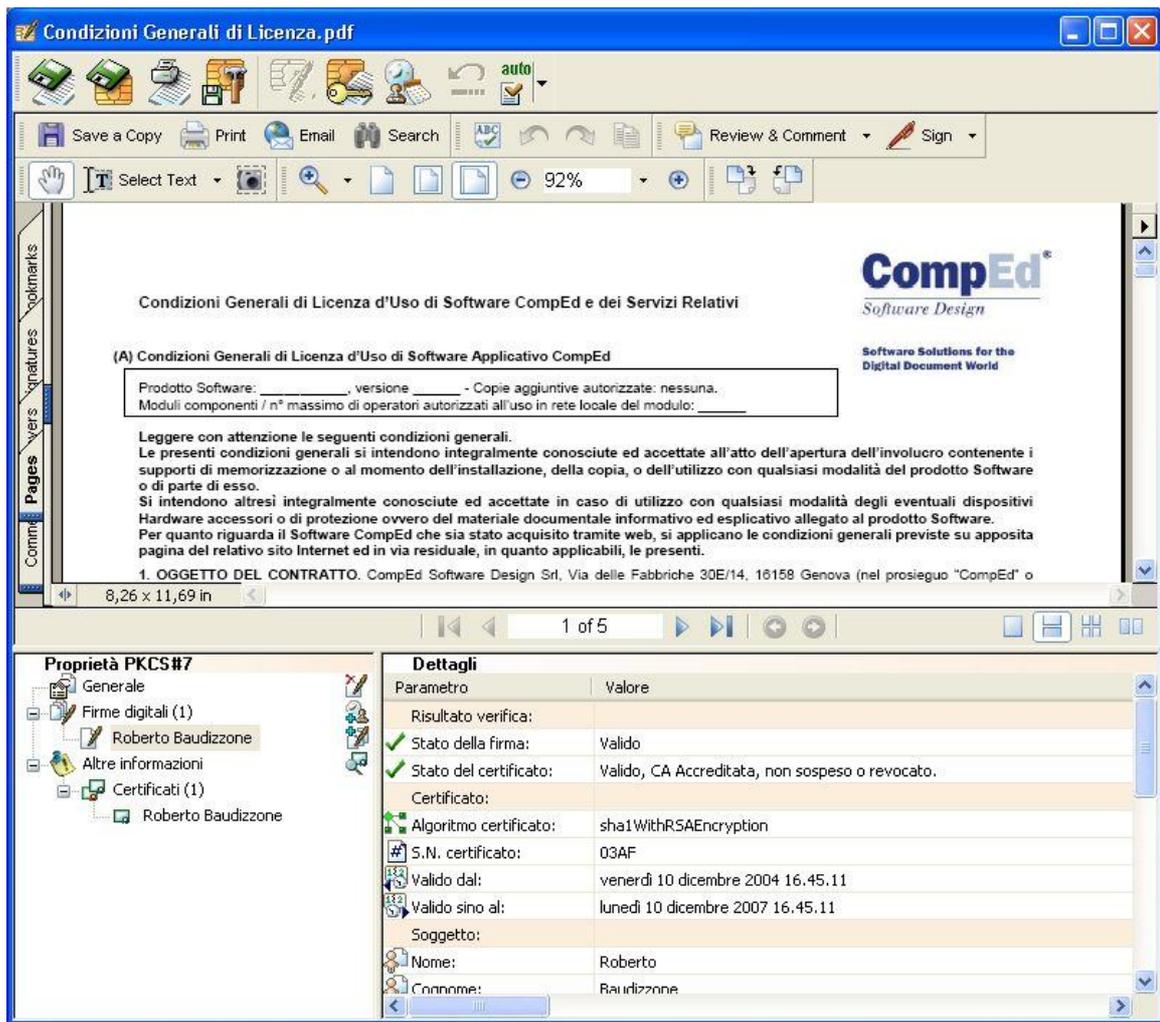
- ***SecurView IMAGING: viewer per documenti in formato grafico "raster"***
  Questo viewer è integrato in DigitalSign. Questo significa che per la visualizzazione di questo tipo di documenti DigitalSign non fa ricorso ad alcuna applicazione esterna, ma solo ad una libreria di gestione di formati grafici (LEAD).
  Il livello di sicurezza è elevato.

Per grafica "raster" si intende una metodologia di rappresentazione delle immagini che si basa sulla visualizzazione di una griglia di punti (detti "pixel", da picture element) di colore (o di intensità di grigio) differente, formando appunto un'immagine.
Esistono molteplici formati per la rappresentazione di immagini in modalità raster. Segue una tabella dei formati supportati dal viewer di DigitalSign, completa dei riferimenti alle specifiche pubbliche:

Estensione per nome file	**Descrizione**	**Conformità ISO**	**Specifiche pubbliche (PAS - Publicly Available Specifications)**
JPEG, JPG	Compressed File Interchange Format	ISO/IEC 10918-4:1999	
TIFF, TIF	Tag image file format for image technology	ISO 12639:1998	
BMP	Microsoft® Windows Bitmap format		http://microsoft.com/
WMF	Microsoft® Windows Metafile Format		http://microsoft.com/
PCX			
PSD	Adobe® PhotoShop Document Format		http://www.adobe.com/
PNG	Portable Network Graphics Format		http://www.libpng.org/pub/png/
TGA	Truevision TARGA Format *)		Truevision, Inc. 7349 Shadeland Station Indianapolis, IN 46256-3925 (317-841-0332 - phone)
EPS	Encapsulated PostScript Format		http://www.adobe.com/
CMP	LEAD Compressed Format		http://www.leadtools.com/

Il Viewer riconosce automaticamente il formato dell'immagine e la visualizza con la corretta interpretazione.

- ***Viewer per documenti di tipo HTML e XML***
  Questo viewer si appoggia su Microsoft Internet Explorer per la visualizzazione dei documenti in formato HTML. In particolare il viewer interfaccia la API di Internet Explorer e non si limita a passare un file temporaneo a tale applicazione, quindi il livello di sicurezza rimane alto, quantunque il formato HTML non sia considerato tanto stabile ed univoco da essere raccomandato per documenti informatici di particolare importanza (a meno di limitarne volutamente il contenuto ad elementi di base del linguaggio).
  La versione minima di Internet Explorer, che deve essere preventivamente installata nel sistema, è la 4.01

NOTA IMPORTANTE: è costume molto diffuso costruire documenti in formato HTML costituiti da testo e immagini, proprio perché questo formato ben si presta ad assemblare diversi oggetti da rappresentare insieme sullo schermo.
Tuttavia un documento firmato in formato PKCS#7 non può contenere più di un file; quindi se il documento HTML contiene riferimenti a immagini, queste non saranno coperte dalla firma digitale. Si deve evitare di firmare digitalmente documenti informatici basati sul formato HTML a meno di essere certi che non contengono immagini o altri oggetti basati su file esterni.

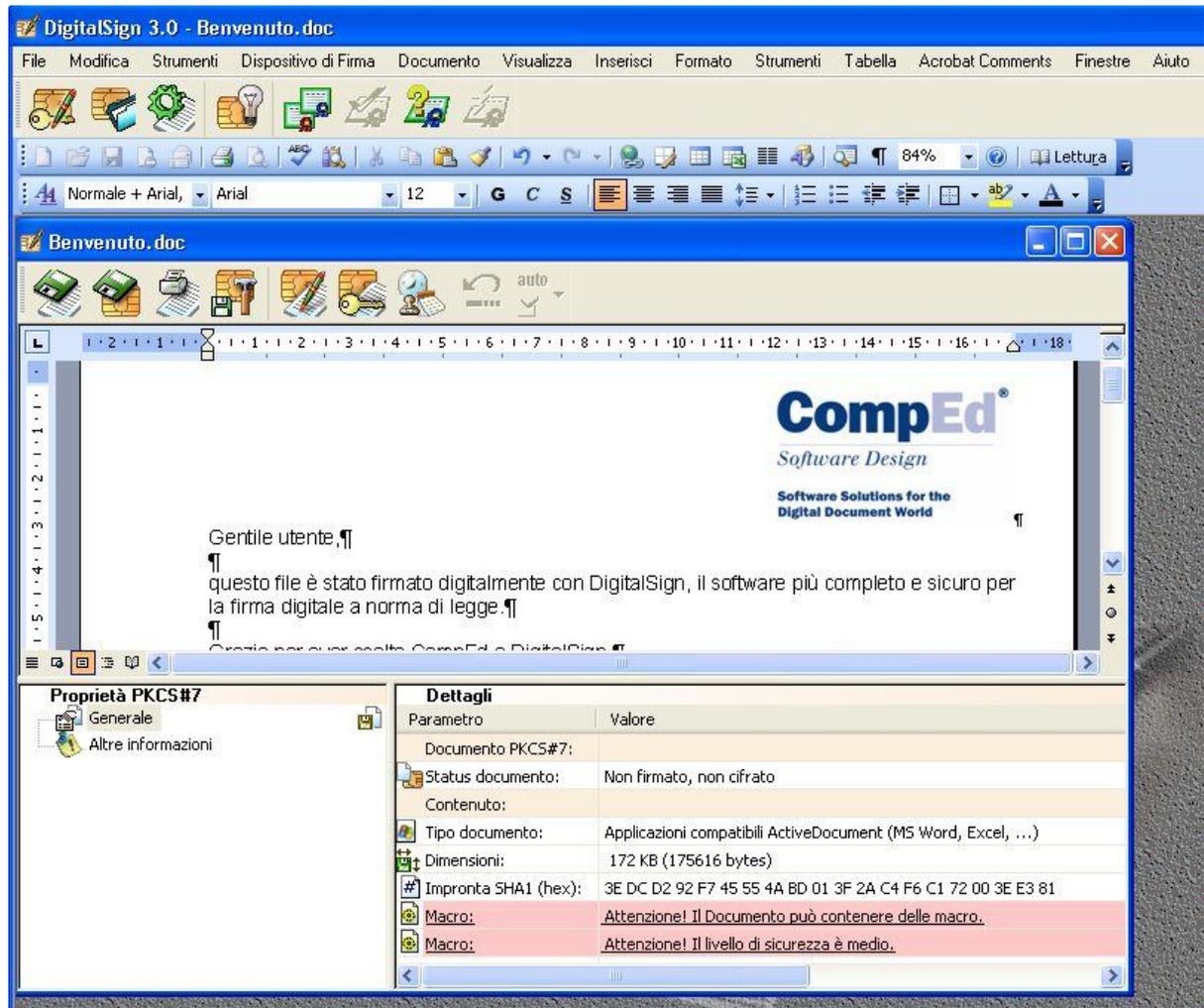
Questo viewer, sotto certe condizioni, viene utilizzato anche per presentare documenti in formato XML (ma senza stylesheet).

Tuttavia, a causa di una gestione della memoria non ottimizzata di Internet Explorer nella presentazione in forma di albero, il sistema può risultare molto rallentato o addirittura collassare – fuori dal controllo di DigitalSign – mentre Internet Explorer tenta la visualizzazione progressiva di grandi documenti XML.
A livello di Opzioni è possibile configurare la massima dimensione per documenti XML; oltre tale soglia il documento verrà presentato con il viewer ASCII.

- ***Viewer per documenti di tipo PDF***
  Questo viewer si appoggia sui servizi messi a disposizione da **Adobe Acrobat ®** o **Adobe Reader ®**, uno dei quali deve essere già presente nel sistema, per la visualizzazione dei documenti in formato PDF all'interno della finestra del viewer stesso.

Il meccanismo di comunicazione tra DigitalSign ed il prodotto di Adobe è diverso secondo la versione di quest'ultimo che si sta usando, per via di diverse tecniche implementate nel tempo dalla Adobe.
In generale DigitalSign comunica con il software Adobe senza la costruzione di file temporanei, ma questo non è vero per le versioni 7.0 di Acrobat e Reader che non consentono altri metodi.
Sul piano della sicurezza la versione 6.0 sarebbe quindi preferibile.

Al menu di DigitalSign si aggiungono un buon numero di comandi e funzioni proprie dell'applicazione Adobe di cui si dispone (si rimanda alla documentazione Adobe)

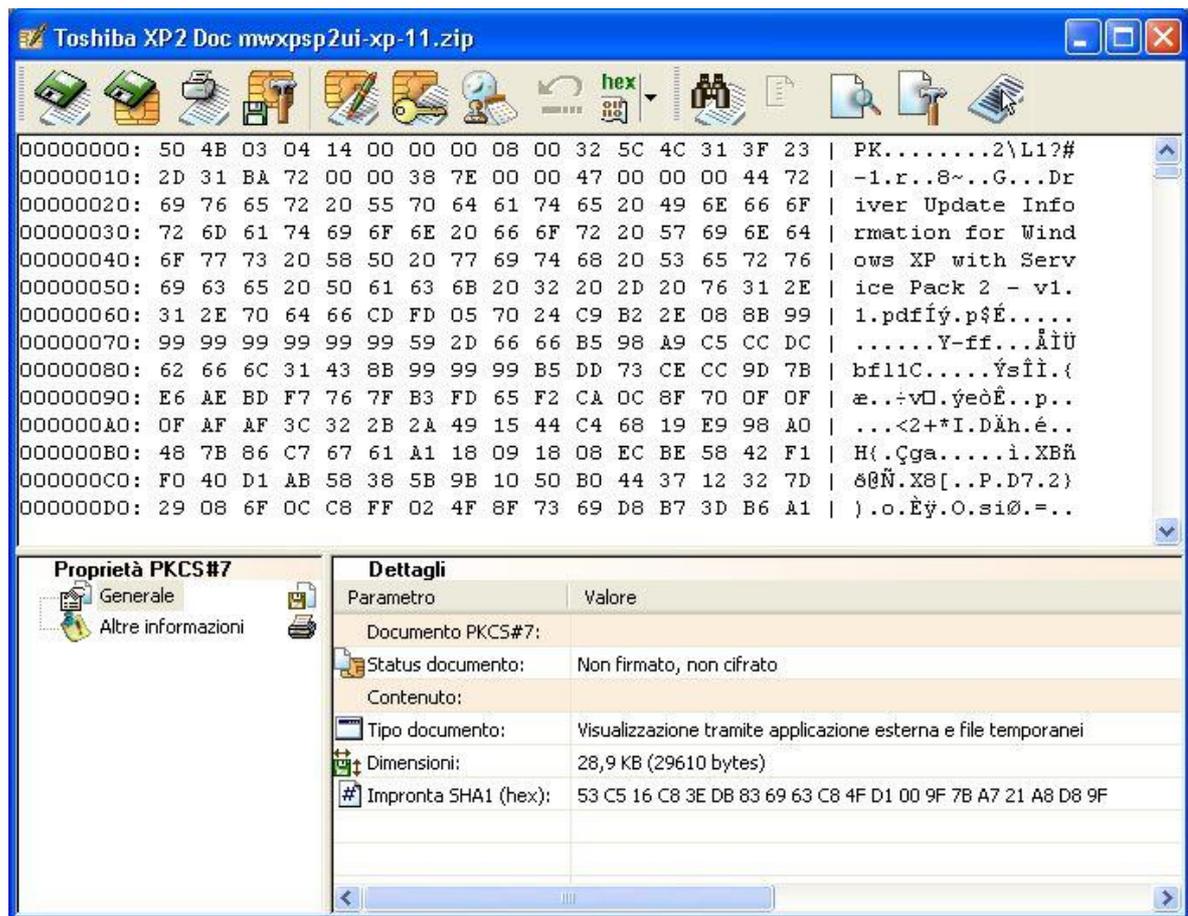
NOTA: il formato PDF, pur essendo considerato tra i più indicati a rappresentare documenti informatici, consente l'inserimento di oggetti variabili (che possiamo definire *macro*) i quali possono in linea di principio introdurre elementi di ambiguità nei documenti stessi, si veda la sezione relativa.

- ***Viewer per applicazioni compatibili ActiveDocument (MS Word, Excel, …)***
  La tecnologia ad oggetti di Microsoft consente di sviluppare applicazione con un profondo livello di integrazione con le applicazioni di Microsoft Office, tramite la proprietà *ActiveDocument*.

DigitalSign sfrutta queste possibilità per gestire documenti elettronici, nei formati normalmente creati e manipolati appunto da queste applicazioni, direttamente dall'interno della finestra documento di DigitalSign.
La comunicazione tra DigitalSign e l'applicazione "server" avviene dunque in maniera profonda, attraverso l'interfacciea COM delle applicazioni, non tramite l'esportazione di file temporanei e il successivo lancio di applicazioni.
In generale questa tecnologia è dedicata ai prodotti Microsoft, ma anche altri produttori possono, in generale, supportare la proprietà ActiveDocument.
Naturalmente lo strumento più "naturale" per l'uso con questo viewer è Microsoft Word.

Si noti che il menu dell'applicazione DigitalSign si arricchisce delle consuete funzioni del menu dell'applicazione utilizzata per gestire il documento contenuto (MS Word nell'esempio).
Il grosso vantaggio di questa tecnologia sta nel fatto che il documento può anche essere **editato** o **addirittura creato da zero** all'interno del viewer, quindi evitando di dover preparare il documento con la propria applicazione e poi aprirlo con DigitalSign al fine di firmarlo digitalmente.

NOTA: i documenti gestiti attraverso queste applicazioni (con particolare riguardo a MS Word ed Excel), permettono di arricchire il testo del documento con oggetti variabili e macro, introducendo un intrinseco rischio di ambiguità nei documenti stessi, si veda la

sezione relativa.

- ***SecurView HEX: dati binari***
  Questo può essere considerato un viewer di emergenza o di controllo.
  Viene automaticamente attivato quando il documento su cui si opera non appartiene ad uno dei formati per i quali DigitalSign possa attivare un viewer specifico e non sia neppure disponibile una applicazione registrata in Windows per la gestione di documenti di quel tipo. Inoltre l'utente può in ogni momento commutare la visualizzazione del viewer corrente in questa modalità, per verificare visivamente i dati binari che costituiscono il documento elettronico

La finestra di visualizzazione presenta i dati, in generale, suddivisi in tre aree (inseribili od escludibili tramite le opzioni relative (…), accessibili attraverso il menu **Strumenti -> Opzioni** e selezionando poi il tab “**Esadecimale**”:

- **colonna indirizzi**: se presente è la colonna più a sinistra. Rappresenta l'offset, in esadecimale, dall'inizio del documento del primo byte della colonna dei dati esadecimali. Poiché la colonna dei dati esadecimali contiene righe di 16 byte, questa colonna procede per incrementi di sedici unità (00000010 in notazione hex)

- **colonna dati esadecimali**: rappresenta il contenuto binario del documento elettronico, espresso in notazione esadecimale

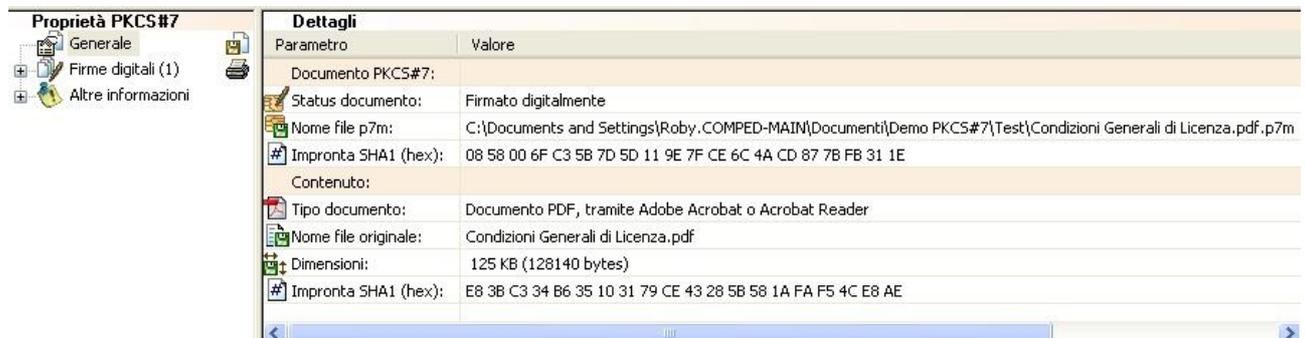
- **colonna dati ASCII:** se presente è la colonna più a destra e rappresenta una interpretazione secondo il codice ASCII dei dati binari, se questa esiste. I valori che non hanno un riferimento "stampabile" nel codice ASCII vengono rappresentati con un punto '.'

4.1.2.2 Finestra documento: area "Proprietà PKCS#7"

Questo riquadro, visualizzato in basso a sinistra nella finestra documento, rappresenta l'insieme degli elementi di informazione che, oltre al documento elettronico, sono contenuti nel file PKCS#7 che rappresenta il documento informatico aperto.

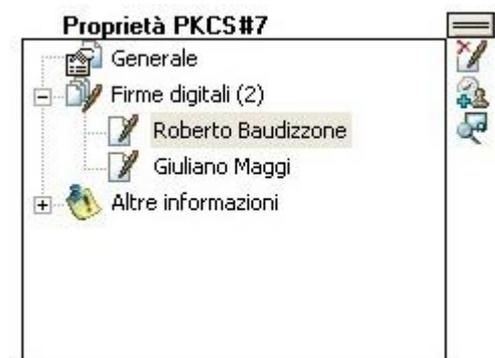
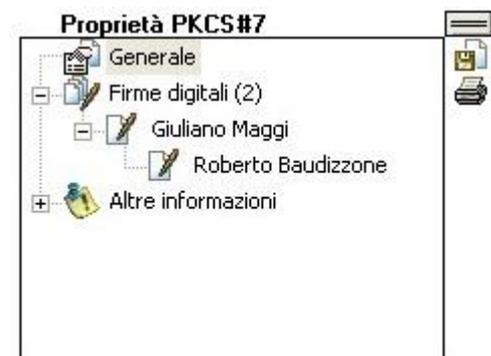
La visualizzazione è presentata come un albero il cui elemento principale è un riepilogo generale. Per gli elementi in cui è riportato il simbolo '+' è possibile agire con il mouse sul simbolo al fine di aprire la visualizzazione del sottoalbero. Analogamente, se è mostrato un simbolo '-', si può richiudere il sottoalbero agendo sul simbolo.

I rami principali dell'albero possono essere:

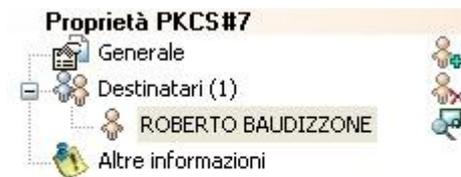
- **Generale**

Questo sottoalbero non può ulteriormente diramarsi e contiene un riepilogo generale del contenuto del documento informatico.
Si tratta dell'unico elemento di un documento PKCS#7 che viene automaticamente compilato al caricamento di un documento non ancora firmato o elaborato in alcun modo.

L'utente può ricavare da questa schermata, tra l'altro, il valore dell'impronta del documento contenuto e, se già salvato sul file, anche l'impronta del documento PKCS#7 complessivo.

- **Firme digitali**
  Questo sottoalbero, se esistente, contiene una o più *foglie*, ciascuna delle quali corrisponde a una firma digitale apposta al documento.
  DigitalSign supporta firme multiple apposte ad un documento, secondo due diverse modalità:

Firme parallele, o congiunte (firme apposte allo stesso livello, riferite al documento, senza reciproci riferimenti tra una firma e l'altra)

Firme gerarchiche, o controfirme (apposte a livelli diversi, una controfirma è riferita alla firma di livello superiore e - solo indirettamente – al documento)

Attestazioni - DigitalSign, dalla versione 3.1, supporta anche "firme deboli" che vengono denominate "Attestazioni", come spiegato nella relativa sezione.
Sul piano pratico questo tipo di firme si presentano con una icona caratteristica, mentre le specifiche più chiare del fatto che non si tratta di una firma a massimo valore legale sono rappresentate nel pannello relativo ai dettagli.

(in questo esempio si nota anche che il certificato usato per questa Attestazione non espone in chiaro il nome e cognome del titolare, ma solo il Codice Fiscale. Del resto l'attestazione può essere basata su certificati che non sono vincolati al rispetto delle linee guida per la firma digitale)

- **Destinatari di cifratura**

Questo sottoalbero, se esistente, contiene una o più *foglie*, ciascuna delle quali corrisponde a un destinatario di cifratura associato al documento.
Si ricordi che se questa lista di destinatari è vuota il documento non viene cifrato e rimane in chiaro.
Con l'aggiunta di un primo destinatario alla lista l'autore del messaggio viene automaticamente aggiunto a sua volta, per consentirgli di riaprire il documento.
Ogni destinatario è mostrato da un simbolo seguito dal nominativo del destinatario

- **Marche temporali**

Questo sottoalbero, se esistente, contiene una o più *foglie*, ciascuna delle quali corrisponde a una marca temporale già associata al documento.

- **Altre informazioni**

In questa sezione dell'albero trovano posto, normalmente, i certificati: ad ogni firma è necessariamente associato un certificato, qui è possibile ispezionarne tutti i dettagli. Opzionalmente è possibile includere nel documento firmato anche una copia della CRL (Lista di Sospensione e Revoca); lo scopo di tale inclusione, seguita dalla marcatura temporale, è di corredare il documento firmato di un set di elementi di prova per attestare che il certificato usato per la firma era valido in un istante di tempo certo.

Il lato destro di questo pannello ospita una *toolbar* verticale attraverso la quale l'utente può accedere rapidamente alle operazioni possibile, senza dover utilizzare il menu o le *toolbar* della finestra principale.
Naturalmente le operazioni possibili variano secondo il tipo di elemento correntemente selezionato. Passando con il cursore sulle relative icone si ottiene una spiegazione di ogni funzione.

Le stesse funzioni sono anche disponibili tramite un "pop-up" menu che appare agendo con il tasto destro su un elemento della finestra:

4.1.2.3 Finestra documento: area "Dettagli"

Questo riquadro della finestra documento mostra in generale una tabella in due colonne nella quale sono rappresentate le informazioni di dettaglio disponibili per l'oggetto correntemente selezionato nell'area proprietà PKCS#7.

L'esempio che segue mostra il contenuto completo di questo riquadro quando visualizza i dettagli di una **firma digitale**:

Dettagli

Parametro	Valore
Risultato verifica:	
Stato della firma:	Valido
Stato del certificato:	Valido, CA Accreditata, non sospeso o revocato.
Certificato:	
Algoritmo certificato:	sha1WithRSAEncryption
S.N. certificato:	0BA6
Valido dal:	martedì 6 settembre 2005 9.42.31
Valido sino al:	mercoledì 6 settembre 2006 9.42.25
Soggetto:	
Nome:	ROBERTO
Cognome:	BAUDIZZONE
Codice fiscale:	BDZRRT62C04D969W
Data di nascita:	04-03-1962
Ruolo:	<non disponibile>
Paese:	IT
Certificato emesso da:	
Nome:	I.T. Telecom FirmaSicura CA, I.T. Telecom S.R.L., IT
Paese:	IT
Firma documento:	
Algoritmo di firma:	RSA-sha1 (1024)
Firma digitale (hex):	3919 A7E1 3CEF 8921 B621 E48D AAAE D8A9 9EC7 F800 9A04 A9E2 2C90 DE0D E990 92AD I
Attributi 'signed':	
contentType	pkcs7-data
signingTime	20/01/06 14.26.49 GMT
messageDigest	B7 54 5F 58 96 CE F8 F2 C6 FD 54 7C 4F 95 9F 81 2E A7 0B B7
Attributi 'unsigned':	
unstructuredName	PKCS7-File-HeaderDescription=Test firma;Filename=MEMO CONFIDENZIALE.txt;

4.1.3 La barra menu di DigitalSign

La barra menu principale di DigitalSign raggruppa i menu di comandi e funzioni accessibili all'utente.

La barra principale contiene le seguenti funzioni (descritte in dettaglio nella sez. 4.2 e successive)

File
Strumenti
Dispositivo di Firma
Finestre
Aiuto

Quando è aperta una finestra documento può essere disponibile anche un altro menu:

Documento

Se la finestra documento si basa su un'altra applicazione per la visualizzazione del documento (per esempio **MS Word ®**) la barra menu si arricchisce di altri menu specifici dell'applicazione.

4.1.4 Le barre strumenti *(toolbar)*

Le toolbar di DigitalSign sono configurabili da parte dell'utente e contengono alcuni bottoni dall'aspetto grafico corrispondenti alle funzioni di uso più comune, normalmente accessibili attraverso il menu.

L'aspetto effettivo delle toolbar dipende dall'edizione di DigitalSign a disposizione, dalle funzioni abilitate al momento, dal tipo di documento eventualmente aperto e selezionato, dalla disponibilità o meno di un dispositivo di firma inserito, dalle caratteristiche dello stesso dispositivo.

Passando con il puntatore del mouse sopra una icona di una toolbar si visualizza un tooltip che richiama l'associata voce del menu:

Le toolbar sono configurabili attraverso il menu **Strumenti -> Opzioni**, scegliendo poi il tab "Toolbar" che conduce ad una apposita finestra di configurazione.

4.1.5 I Pannelli Informativi

Nella finestra principale di DigitalSign possono essere visualizzati (per tramite del menu Finestre) alcuni pannelli di informazione, che a loro volta possono essere chiusi o aperti agendo sul simbolo a forma di freccia.

Questi pannelli consentono soltanto di visualizzare rapidamente alcune informazioni relative alla configurazione corrente del dispositivo di firma e delle opzioni di *security* impostate, ma non permettono di modificare direttamente tali informazioni.
Si noti che la voce File System può non comparire, se è inserito un dispositivo di firma di tipo PKCS#11.

L'illustrazione sopra riportata mostra i pannelli tutti in posizione chiusa. Operando sul simbolo a destra è possibile aprire (o richiudere) tutti i pannelli.

I pannelli disponibili sono:

- **Lettore e smartcard**

Questo pannello mostra alcuni dettagli relativi al lettore di smartcard correntemente attivo, all'eventuale modulo PKCS#11 tramite cui avviene il collegamento al dispositivo, alla particolare smartcard inserita nel lettore

- **File System**

Questo pannello mostra alcuni dettagli relativi ai dati memorizzati sul dispositivo di firma, nell'ipotesi che si tratti di un dispositivo interfacciato a livello APDU e che sia stato inizializzato mediante la **Personal Certification Authority** di DigitalSign.
Il pannello non è visibile se DigitalSign è configurato ad operare con dispositivi interfacciati in modalità PKCS#11.

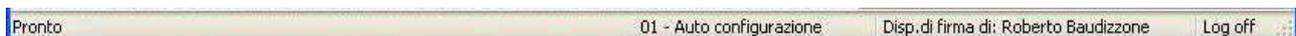
- **Titolare Smartcard**

Questo pannello mostra alcuni dettagli sull'identità del titolare del dispositivo di firma correntemente inserito nel lettore. I dati visualizzati sono estratti dal certificato letto dal dispositivo stesso.

- **Opzioni di Sicurezza**

Questo pannello mostra le informazioni principali relativamente alle opzioni di *security* correntemente attive.
Per modificare la configurazione di tali opzioni si utilizza il menu **Strumenti -> Opzioni di Security**

4.1.6 La barra di stato

La barra di stato principale di DigitalSign viene mostrata alla base della finestra principale dell'applicazione

Come si può notare la status bar principale mostra informazioni relative allo stato di funzionamento di DigitalSign, alla modalità di gestione dell'interfaccia al dispositivo di firma, al titolare del dispositivo di firma correntemente inserito, allo stato di *Logon* o di *Logoff* del dispositivo stesso.

4.2 Il menu "File"

Questo menu contiene diverse funzioni, alcune delle quali possono non essere disponibili, per esempio se nessun documento è aperto.
Oltre alle funzioni descritte nelle sezioni seguenti, è di norma presente – come illustrato in figura – anche una lista di elementi corrispondenti agli ultimi 5 documenti elaborati, utili per aprire in modo immediato un documento utilizzato di recente.

Gli elementi di menu sono visualizzati accanto al simbolo dell'eventuale icona della barra strumenti che esegue la stessa funzione.

4.2.1 Log On / Log Off

Funzione non disponibile con DigitalSign Reader

Questa funzione di menu consente di porre il dispositivo di firma (la smartcard) in uno stato di "Log On", ossia di attivarne tutte le funzioni previa introduzione del proprio codice riservato, mediante una apposita finestra di dialogo.

La funzione non è utilizzabile se nessun dispositivo di firma è inserito.

Se il dispositivo è già in tale stato di Logon questa funzione lo pone in stato di Logoff, disattivandone le funzioni.

La voce di menu mostra la dicitura **Log On** se il dispositivo è disattivo, oppure **Log Off** se il dispositivo già è attivo.

4.2.2 Controllo licenze

Questa funzione è abilitata soltanto nelle edizioni di DigitalSign fornite in package con altri prodotti CompEd, come Legal Document System ®, o più in generale nei contesti in cui esiste un sistema centralizzato di controllo della licenza d'uso (CompEd License Manager.

Scopo di questa funzione è visualizzare lo stato della licenza d'uso.

4.2.3 Nuovo Documento

Funzione non disponibile con DigitalSign Reader

Permette all'utente di generare dal nulla un nuovo documento e di incapsularlo in una busta crittografica (*envelope* PKCS#7), pronta per la composizione del contenuto e per la successiva firma, cifratura, marcatura temporale, ecc.

In generale, tramite questa funzione, il documento viene appunto generato ex novo. Questo è possibile solo utilizzando – per la composizione del contenuto – applicazioni che supportino la modalità ActiveDocument (tipicamente le applicazioni di Microsoft © Office, quali Word, Excel, ecc.)
All'utente viene presentata una piccola finestra di dialogo per la selezione dell'applicazione da usare, cioè del tipo di documento da creare:

La lista delle applicazioni utilizzabili per questa operazione si controlla e configura mediante il menu **Strumenti -> Opzioni** ed agendo sul tab **ActiveDocument** ottenendo così una specifica schermata di configurazione.
La finestra documento risultante, che nell'area viewer contiene un'istanza dell'applicazione selezionata, attiva con un documento vuoto, può essere usata direttamente per scrivere il documento.
Naturalmente, dopo che si sarà apposta una firma, il documento non dovrà più essere toccato (altrimenti il sistema genererà adeguati messaggi di avviso).

L'ultima opzione **Seleziona file esistente** consente invece di caricare un documento già esistente in un nuova busta crittografica, ottenendo un effetto analogo a quello che si otterrebbe usando la funzione **Apri Documento** applicata ad un documento che non sia in formato PKCS#7.

In particolare, questa modalità deve essere usata quando si voglia creare un documento "a cipolla": anche se non è un procedimento particolarmente raccomandato, alcuni utenti vogliono poter apporre una firma digitale ad un documento che è già a sua volta un PKCS#7 firmato.

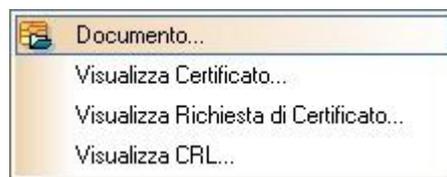
4.2.4 Incolla come Nuovo Documento

Funzione non disponibile con DigitalSign Reader

Genera un nuovo documento PKCS#7 il cui contenuto è ricavato dal contenuto degli appunti (la *clipboard*).

La voce del menu è accessibile solo se negli appunti è presente del testo utilizzabile con una funzione di tipo “incolla”.

È una funzione particolarmente comoda per creare rapidamente documenti firmati contenenti frammenti di testo copiati da altre finestre, per esperimenti e prove.

4.2.5 Il sottomenu “Apri”

Questo sottomenu conduce ad alcune funzioni specifiche per aprire/visualizzare documenti di diverso tipo

4.2.5.1 Documento

Presenta una finestra di dialogo standard per la selezione di un file da aprire.
La posizione di partenza per la selezione del file dipende dalle impostazioni dei percorsi di lavoro, configurabili tramite il menu **Strumenti -> Opzioni** ed agendo sul tab **Percorsi**.

Se si apre un documento già in formato di busta crittografica allora il documento viene aperto così come si trova; se invece si apre un documento “normale” (es. PDF, DOC, TXT, JPG, ecc.) si creerà una nuova busta crittografica contenente tale documento, pronto per le successive operazioni di firma, cifratura, marcatura temporale, ecc.

Si noti che questa funzione ha un comportamento flessibile: applicandola a documenti di tipologia particolare per DigitalSign (es. Certificati, Liste di Sospensione e revoca, ecc.) essi verranno aperti con gli appropriati moduli di presentazione, non nella finestra documento, esattamente come se venissero usate le funzioni descritte nelle prossime sezioni.

4.2.5.2 Visualizza certificato

Permette di visualizzare il contenuto di un certificato, previa selezione del file, attraverso il modulo standard di visualizzazione.

4.2.5.3 Visualizza Richiesta di Certificato

Permette di visualizzare il contenuto di una Richiesta di Certificato PKCS#10, previa selezione del file, attraverso lo stesso modulo standard di visualizzazione che normalmente si usa per visualizzare il contenuto di un certificato.

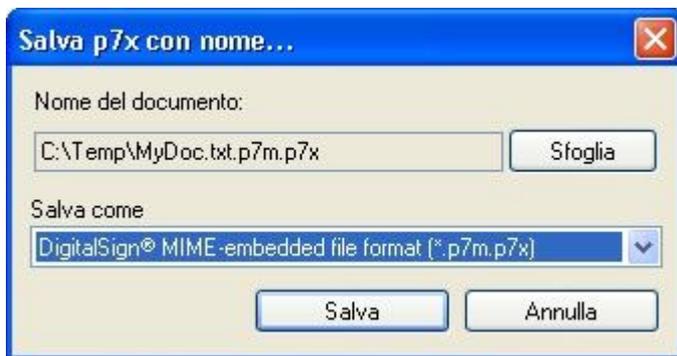
4.2.5.4 Visualizza CRL

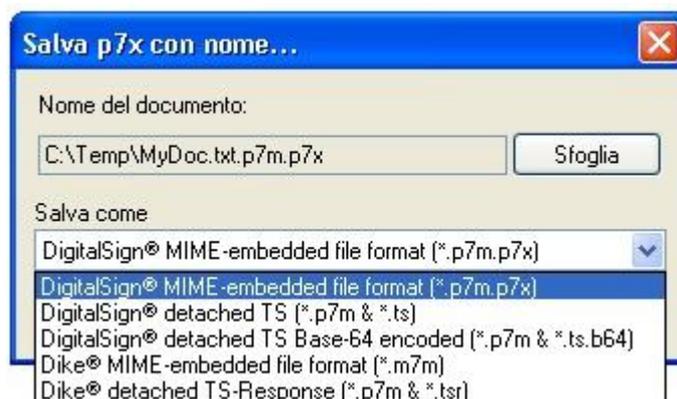
Permette di visualizzare il contenuto di una Lista di Sospensione e Revoca disponibile su un file, attraverso uno specifico modulo di visualizzazione.

4.2.6 Salva Documento

Permette di salvare su disco il documento su cui si sta lavorando.
In generale si produce un file in formato **.p7m**, ossia una busta crittografica PKCS#7.
Se il documento non era ancora stato salvato in precedenza il sistema presenta una finestra di dialogo standard per l'impostazione del nome del file su cui scrivere. La posizione di partenza per la selezione del file dipende dalle impostazioni dei percorsi di lavoro, configurabili tramite il menu **Strumenti -> Opzioni** ed agendo sul tab **Percorsi.**

Se il documento era già stato salvato prima DigitalSign lo salva direttamente (cioè non chiede il nome), ma nel caso – probabile – che il file sia già esistente chiede conferma della volontà di sovrascriverlo.

Se il documento in questione è marcato temporalmente è necessario un passaggio in più, perché esistono diverse forme in cui è possibile rappresentare un documento di questo tipo. L'utente vedrà una finestra di dialogo di questo genere:

L'utente può usare il bottone Sfoglia per scegliere la posizione ed il nome del file da creare, quindi completare o annullare l'operazione.

La lista permette di scegliere tra le diverse modalità disponibili:

Per una descrizione delle diverse modalità si veda la sezione relativa.

4.2.7 Salva Documento con Nome

Funzione assolutamente analoga alla precedente, ma permette di scrivere un file di nome differente rispetto all'originale.

4.2.8 Salva Contenuto

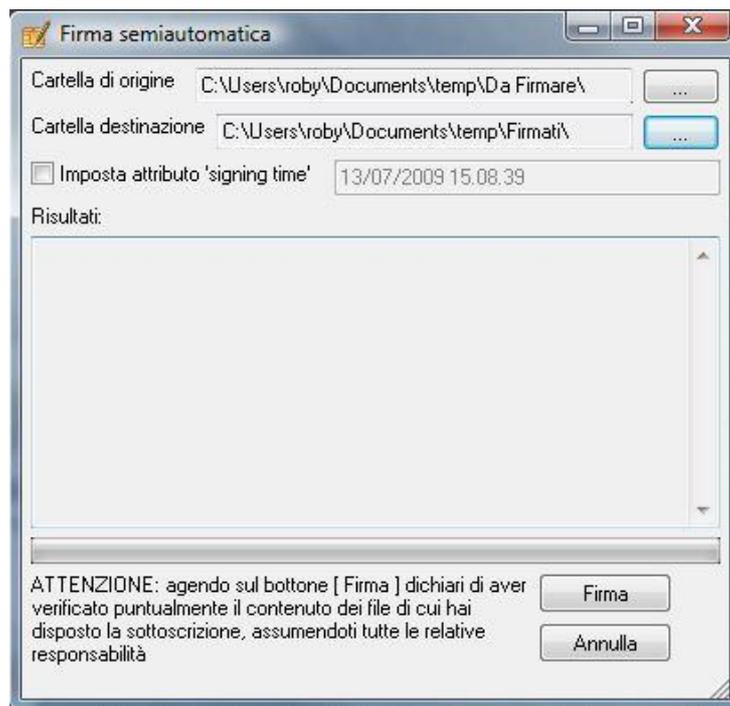
Questa funzione consente di salvare su disco una copia del documento contenuto nella busta crittografica su cui si sta operando.

Se, per esempio, l'utente apre il documento **`proposta_di_contratto.pdf.p7m`**, ossia un documento in formato **pdf** firmato digitalmente e quindi racchiuso in una busta crittografica PKCS#7, questa funzione permette di salvare una copia del documento **`proposta_di_contratto.pdf`**.

Il sistema presenta una finestra di dialogo standard per l'impostazione del nome del file su cui scrivere. La posizione di partenza per la selezione del file dipende dalle impostazioni dei percorsi di lavoro, configurabili tramite il menu **Strumenti -> Opzioni** ed agendo sul tab **Percorsi.**

4.2.9 Firma Contenuto Cartella

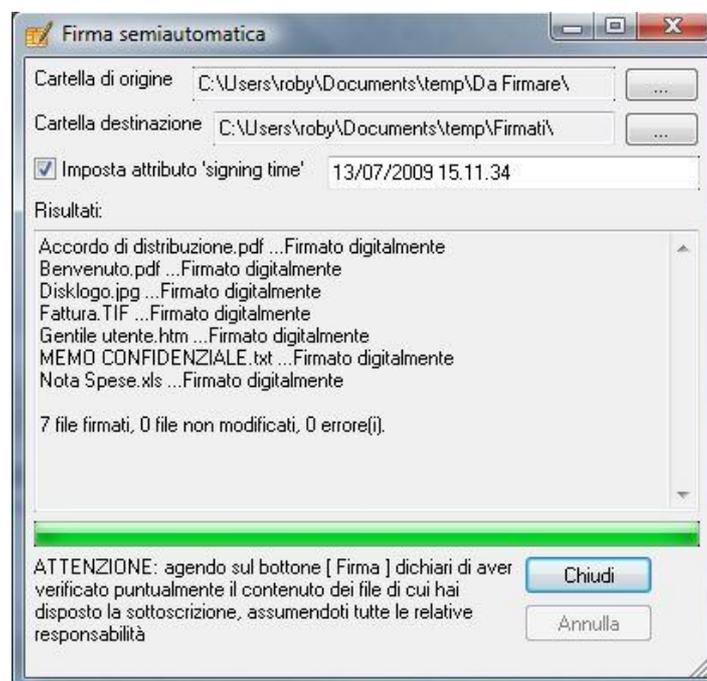
Funzione non disponibile con DigitalSign Reader

Questa funzione consente di applicare una firma digitale a tutti i documenti presenti in una cartella selezionata dall'utente e salvare il risultato in una seconda cartella.
Appare questa finestra di dialogo:

L'utente deve selezionare, mediante i due bottoni **[…]** associati a **Cartella di origine** e **Cartella destinazione**, le cartelle su cui operare.
Al momento in cui si agisce sul bottone Firma si avvierà un processo semiautomatico di firma di tutti i documenti contenuti nella cartella di origine. I documenti risultanti verranno copiati nella cartella di destinazione.
Opzionalmente è possibile spuntare il checkbox **Imposta attributo 'signing time'**: i documenti firmati avranno tale attributo attivato, ossia risulterà la data ed ora di apposizione della firma.

Si noti che:

- le cartelle di origine (dei file da firmare) e quella di destinazione (dei file firmati) devono essere distinte
- se un documento da firmare risulta già firmato da un diverso soggetto (più esattamente, se già esiste una firma apposta con un certificato diverso da quello in uso) verrà aggiunta la firma dell'utente, in modo parallelo;
- se se un documento da firmare risulta già firmato dallo stesso utente, il documento non viene rifirmato e resta inalterato

NOTA IMPORTANTE: questa procedura semiautomatica si basa sul presupposto che l'utente abbia già visionato con cura i documenti che sottopone al processo di firma e che agendo sul bottone **Firma** si assuma la responsabilità effettiva di apporre la propria firma digitale.

Durante il processo la finestra mostra i progressi, file per file, mostrando eventuali errori e comunque il risultato dell'operazione. Al termine apparirà una situazione di questo tipo:

Si noti che questa funzione è ottenibile anche operando dalla shell di Windows, si veda questa sezione.

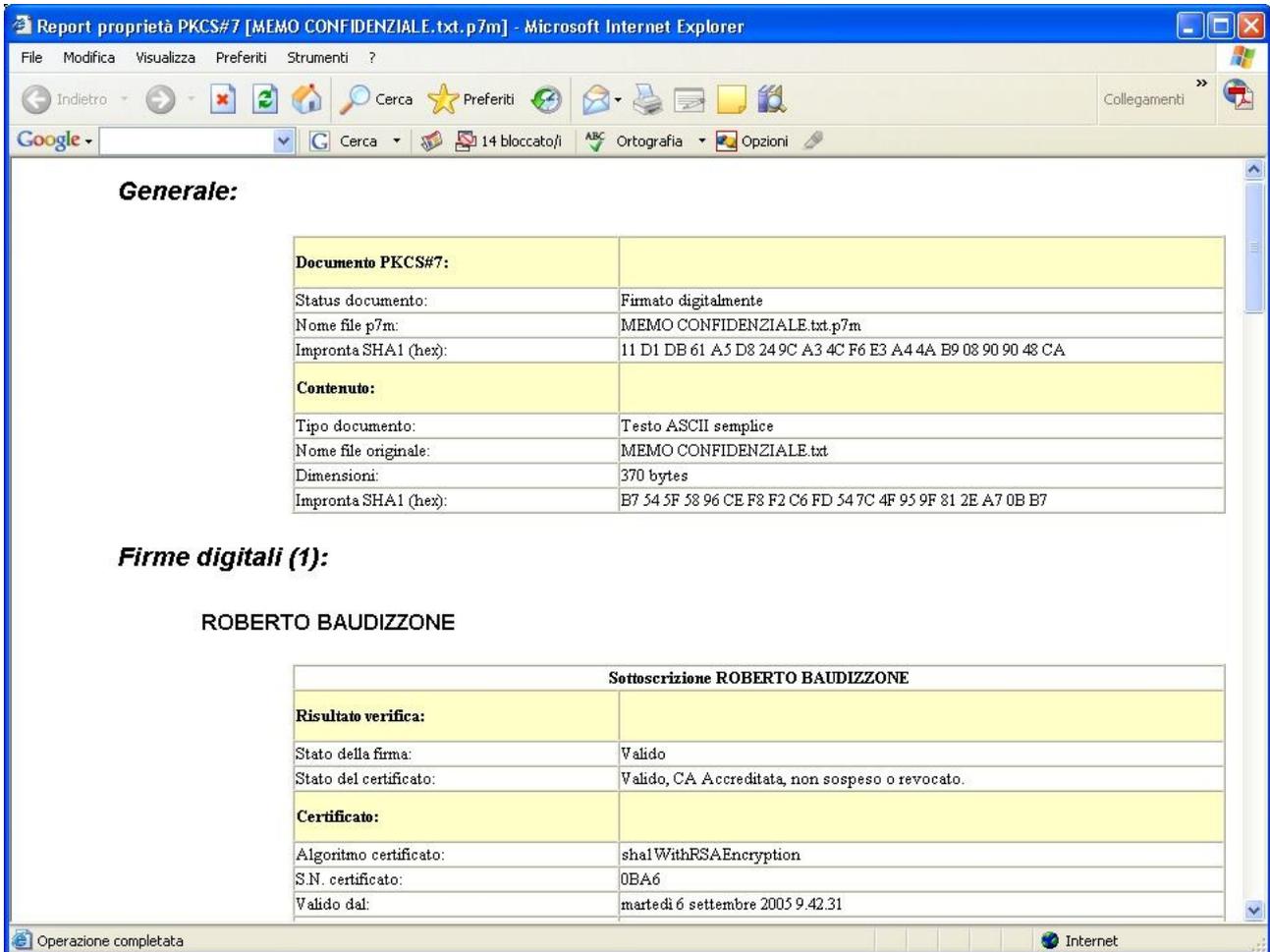
4.2.10 Stampa

Manda in stampa il documento su cui si sta operando.

Viene presentata una finestra di dialogo standard per il controllo del processo di stampa (scelta del dispositivo, scelta dell'intervallo di pagine, ecc.)

4.2.11 Genera Report PKCS#7

Questa funzione consente di generare un rapporto contenente tutti i dettagli relativi al documento correntemente aperto, inclusi il valore dell'impronta, la firma o le firme digitali presenti, i certificati, le marche temporali, ecc.

Questo report è costruito in formato HTML e viene successivamente aperto tramite Internet Explorer, da cui è possibile salvarlo, stamparlo, ecc.

Report proprietà PKCS#7 [MEMO CONFIDENZIALE.txt.p7m] - Microsoft Internet Explorer

Generale:

Documento PKCS#7:	
Status documento:	Firmato digitalmente
Nome file p7m:	MEMO CONFIDENZIALE.txt.p7m
Impronta SHA1 (hex):	11 D1 DB 61 A5 D8 24 9C A3 4C F6 E3 A4 4A B9 08 90 90 48 CA
Contenuto:	
Tipo documento:	Testo ASCII semplice
Nome file originale:	MEMO CONFIDENZIALE.txt
Dimensioni:	370 bytes
Impronta SHA1 (hex):	B7 54 5F 58 96 CE F8 F2 C6 FD 54 7C 4F 95 9F 81 2E A7 0B B7

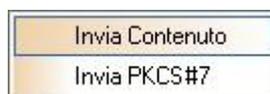
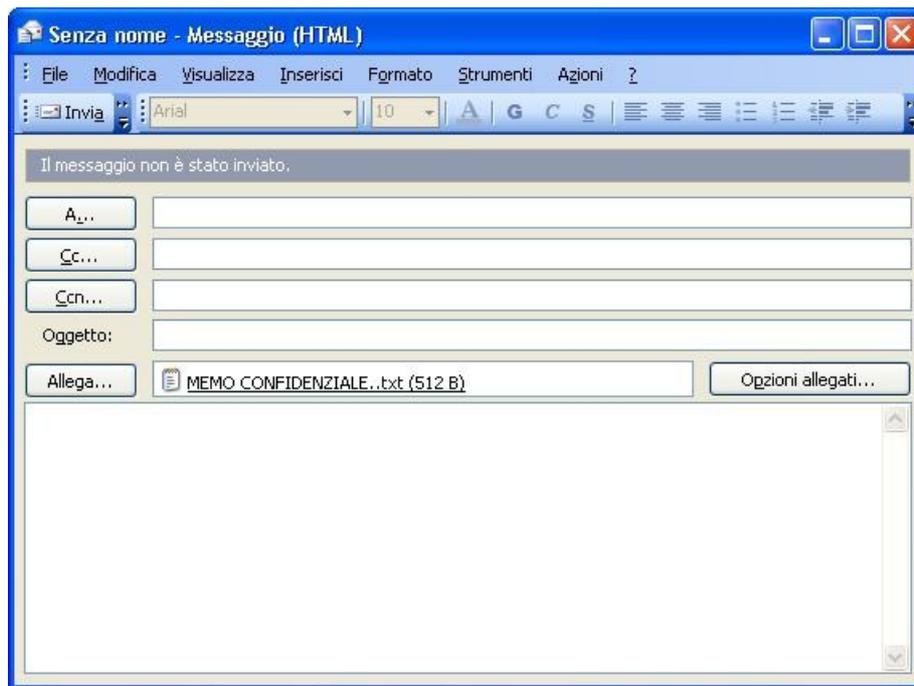
Firme digitali (1):

ROBERTO BAUDIZZONE

Sottoscrizione ROBERTO BAUDIZZONE	
Risultato verifica:	
Stato della firma:	Valido
Stato del certificato:	Valido, CA Accreditata, non sospeso o revocato.
Certificato:	
Algoritmo certificato:	sha1WithRSAEncryption
S.N. certificato:	0BA6
Valido dal:	martedì 6 settembre 2005 9.42.31

Operazione completata — Internet

4.2.12 Il sottomenu "Invia Email"

Presenta un sottomenu con due opzioni successive:

È necessario che sul sistema sia impostato un client predefinito di posta elettronica; tramite tale client (es. **MS Outlook ®**) viene creato un nuovo messaggio di posta elettronica contenente l'oggetto selezionato come allegato.

4.2.13 Registro Attività

Questa funzione è disponibile solo con le edizioni di livello “Professional”, escludendo quindi le edizioni “Reader e “Lite”.

Consente di ispezionare il contenuto del registro delle attività, tramite un componente software separato da DigitalSign, per i cui dettagli si veda la sezione relativa.

Per l’abilitazione/disabilitazione della funzione di registrazione degli eventi e per la configurazione sulle categorie di eventi da includere nella registrazione si usa relativa configurazione si usa il menu **Strumenti -> Opzioni** agendo quindi sul tab **Registro Attività**

4.2.14 Uscita

Questa funzione provoca la chiusura dell’applicazione.

Si noti che la normale azione su questo comando (o sul simbolo di chiusura della finestra principale dell’applicazione) DigitalSign non viene del tutto scaricato dalla memoria e resta quindi pronto per una rapida riattivazione. Questo stato è testimoniato dalla presenza dell’icona di DigitalSign nella *system tray*:

Lo scaricamento dalla memoria avviene spontaneamente dopo qualche minuto di completa inattività di DigitalSign (considerando anche il fatto che altre applicazioni potrebbero utilizzarne i servizi), oppure:

- tenendo premuto il tasto SHIFT quando si attiva questo comando di uscita (o si clicca sul bottone di chiusura della finestra);

- facendo click con il tasto destro sull'icona di DigitalSign presente nella *system tray* dopo la chiusura normale dell'applicazione ed operando sul pop-up menu che appare:

L'elemento evidenziato nella figura è quello della chiusura normale: indica che nessuna applicazione sta utilizzando i servizi di DigitalSign per tramite della sua interfaccia COM e quindi si può chiudere (scaricare dalla memoria) DigitalSign senza problemi.

Se invece qualche applicazione sta usando DigitalSign lo stesso menu si presenterebbe in una forma del genere:

La chiusura sarebbe dunque possibile solo con la **Chiusura forzata**, tenendo presente che questo potrebbe avere effetti negativi sulle altre applicazioni aperte.

In entrambi i casi **Ripristina** riattiva la finestra principale di DigitalSign.

4.3 Il menu "Strumenti"

Il menu Strumenti raccoglie diverse funzioni di servizio ed utili alla configurazione del sistema.

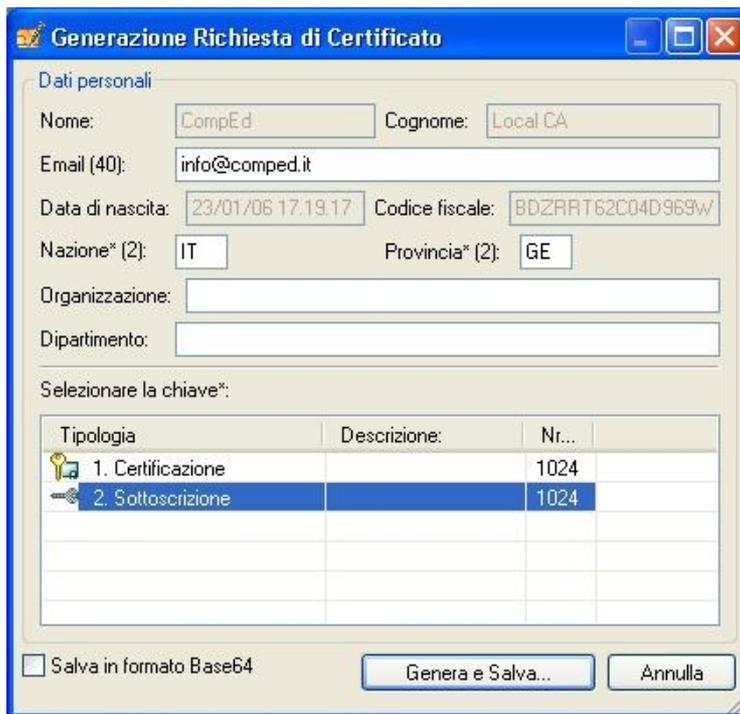
Alcune voci conducono ad ulteriori sottomenu.

4.3.1 Richiesta di certificato PKCS#10

Questa funzione non è disponibile in DigitalSign Reader ed in DigitalSign Lite.
Inoltre può essere disabilitata in alcune edizioni Professional OEM distribuite da alcune importanti organizzazioni.

Questa funzione viene di regola utilizzata nei contesti di utilizzo sperimentale o comunque in un gruppo chiuso di utenti, quando non si intende utilizzare smartcard fornite da un Certificatore Accreditato.

In tali casi si istituisce una funzione di *Certification Authority* che emette certificati per gli altri utenti; questi ultimi devono dal canto loro provvedere alla generazione delle coppie di chiavi sui propri dispositivi e quindi produrre, appunto, le relative "Richieste di Certificato" attraverso questa funzione.
In ogni caso è possibile – salvo limitazioni specifiche presentate da alcune smartcard – generare richieste di certificato anche per coppie di chiavi per i quali già esista un certificato qualificato: si raccomanda la massima attenzione perché l'esistenza di diversi certificati per la stessa coppia di chiavi è una potenziale fonte di ambiguità.

Una volta raggiunto lo stato di Logon del dispositivo viene mostrata una finestra di dialogo:

Nel caso il dispositivo contenga più di una coppia di chiavi occorre naturalmente selezionare quella su cui si intende operare.

- il checkbox **Base64** per effettuare la scrittura del file in tale formato;
- il bottone **Genera e Salva** per avviare l'operazione di generazione del certificato;
- il bottone **Annulla** per tornare allo stato precedente senza eseguire l'operazione.

4.3.2 Gestione DB Locale dei Certificati

Questa voce di menu consente di accedere al modulo di gestione del DB dei Certificati, si veda la sezione dedicata.

4.3.3 Gestione CRL

Questa voce di menu consente di accedere al modulo di gestione delle Liste di Sospensione e Revoca (CRL), si veda la sezione dedicata.

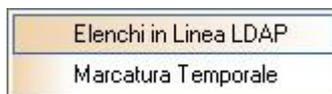
4.3.4 Opzioni di Security

Questa voce di menu consente di accedere al modulo di gestione delle Opzioni di Sicurezza, prevalentemente dedicato alle impostazioni per la verifica di firme e certificati; si veda la sezione dedicata.

4.3.5 Opzioni

Questa voce di menu consente di accedere al modulo di gestione delle Opzioni, attraverso il quale si impostano gran parte dei parametri di configurazione di DigitalSign, si veda la sezione dedicata.

4.3.6 Il sottomenu "Configurazione Servizi"

Questa voce conduce ad ulteriore sottomenu:

- Il primo elemento di questo sottomenu apre il modulo di configurazione degli elenchi di certificati in linea LDAP, si veda la sezione dedicata.

- Il secondo elemento conduce alla configurazione dei servizi di marcatura temporale, si veda la sezione dedicata.
  Funzione non disponibile in DigitalSign Reader

4.3.7 Personal Certification Authority

Questa funzione – insieme a tutte le funzioni del relativo sottomenu - non è disponibile in DigitalSign Reader ed in DigitalSign Lite.
Inoltre può essere disabilitata in alcune edizioni Professional OEM distribuite da alcune importanti organizzazioni.

NOTA: CompEd ha realizzato una specifica guida, separata da questo manuale utente, per assistere l'utente nell'utilizzo della Personal Certification Authority. È possibile richiederle tale guida direttamente a CompEd.

Questa voce conduce ad ulteriore sottomenu:

La **Personal Certification Authority** è un sottosistema integrato in alcune edizioni di DigitalSign che consente di riprodurre, in un ambito circoscritto, le funzionalità di una vera e propria *Certification*

Authority, allo scopo di personalizzare smartcard vergini e generare – in totale autonomia – certificati e liste di revoca.

NOTA IMPORTANTE: lo scopo essenziale della Personal Certification Authority è quello di produrre certificati, da utilizzare in ambito sperimentale oppure da una organizzazione che non ha necessità del massimo valore legale ottenibile usando certificati qualificati rilasciati da un Certificatore Accreditato.
Nel caso si desideri che la nostra CA provveda anche alla gestione delle operazioni di revoca dei certificati occorre predisporre un indirizzo (URL) a cui rendere accessibile la copia aggiornata della Lista di Revoca (CRL), così che i *client* possano consultarla in fase di verifica firme e certificati.
Ogni certificato emesso da una CA contiene a tal fine un attributo “CRL Distribution point” (CDP) che rappresenta proprio tale indirizzo.
DigitalSign dovrebbe essere configurato in modo da inserire il giusto CDP in tutti i certificati che produce. A tal fine esiste una specifica sezione del file .INI (un file di configurazione che si trova nella stessa cartella dell’eseguibile e ne porta il nome – per esempio DigitalSignPro.INI nel caso dell’edizione Professional standard – con l’estensione .INI.
La sezione di questo file interessata al CRL Distribution Point è quella evidenziata qui sotto, in cui occorre indicare l’esatta URL che verrà riportata nei certificati:

```
...
#==========================#
#  certificate extensions  #
#==========================#
[ cert_ext ]
crlDistributionPoints=URI:http://gateway.comped.it/temp/test_ca.crl
certificatePolicies=ia5org,1.3.6.1.5.5.7.2.1,@polsect

[ polsect ]
policyIdentifier = 1.3.5.8
CPS.1="http://my.host.name/"
CPS.2="http://my.your.name/"
userNotice.1=@notice

[ notice ]
explicitText="Explicit Text Here"
organization="Organization Name"
noticeNumbers=1,2,3,4
...
```

La produzione delle CRL si gestisce poi attraverso il modulo descritto nella sezione dedicata.

4.3.7.1 Generazione certificato Root (o Certificato di CA)

Questa funzione agisce su una coppia di chiavi, di tipologia “Certificazione”, già creata nel dispositivo e genera per tale coppia di chiavi un certificato di CA.

Viene mostrata questa finestra di dialogo:

L'utente deve indicare il nome ed il percorso del certificato da produrre, eventualmente utilizzando il bottone **[…]** che permette di sfogliare il *file system*.

Il periodo di validità va espresso in giorni. Per certificati basati sulle normali smartcard, con chiavi di 1024 bit, si raccomanda una durata di 2 anni (730 giorni), emettendo poi certificati d'utente della durata di 1 anno solo per il primo anno di validità di questo certificato.

- Il checkbox **Base64** provoca la scrittura del certificato in tale formato
- Il bottone **Genera** avvia l'operazione
- Il bottone **Annulla** torna allo stato precedente senza eseguire l'operazione

Il certificato viene generato immediatamente, quindi viene presentata la finestra standard per la visualizzazione del contenuto del un certificato appena generato.

Si noti che per poi utilizzare il dispositivo di firma al fine di emettere altri certificati sarà necessario caricare nella memoria del dispositivo stesso il certificato appena creato. Si veda in proposito la gestione dei certificati *on-board*.

4.3.7.2 Generazione Certificato

Nell'ipotesi di avere attivato (inserito) un dispositivo di firma contenente una coppia di chiavi della tipologia di "Certificazione" e di avere a disposizione il relativo certificato di CA (cioè quello di tipo "Root" associato alla coppia di chiavi di Certificazione), permette di generare un certificato in risposta ad una Richiesta di Certificato.

Si osservi che il meccanismo è il seguente:

1. il soggetto titolare di una coppia di chiavi di cui richiede un certificato deve generare una **richiesta di certificato**.
   In alcuni contesti, sensibili sul piano della sicurezza, l'operazione di generazione dovrebbe avvenire alla presenza di un incaricato dell'ente che emette il certificato. Questo allo scopo di assicurarsi dell'identità del richiedente e sul fatto che la coppia di chiavi risieda in un dispositivo di firma di tipo approvato;
2. la richiesta di certificato conterrà i dati anagrafici e copia della chiave pubblica; quindi sarà firmata con la chiave privata della coppia oggetto della richiesta di certificato;
3. in fase di emissione di certificato si useranno i dati anagrafici e la chiave pubblica della richiesta, dopo aver verificato la firma usando la chiave pubblica stessa (questo per assicurarsi che il richiedente sia veramente in possesso della chiave privata.

Per la generazione di un certificato viene mostrata questa finestra di dialogo:

L'utente deve selezionare il file di origine (una richiesta di certificato PKCS#10, si veda la sezione relativa) ed indicare il nome del file del certificato da generare, eventualmente sfogliando il file system utilizzando i bottoni **[…]**.

Va indicata anche la durata di validità del certificato prodotto, avendo cura che tale durata non ecceda il termine di validità del certificato di CA.

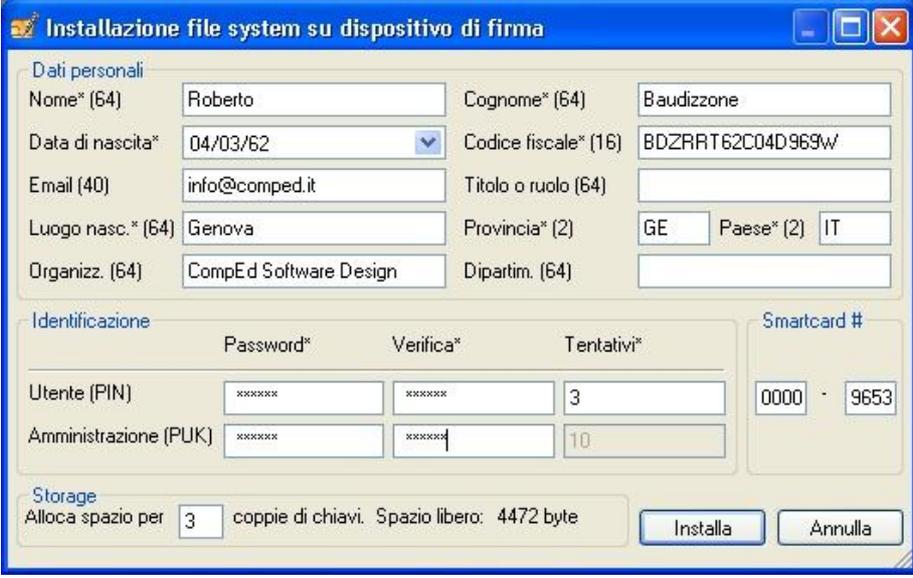
- Il checkbox **Base64** provoca la scrittura del certificato in tale formato
- Il bottone **Genera** avvia l'operazione di generazione del certificato.
- Il bottone **Annulla** torna allo stato precedente senza eseguire l'operazione.
- Il bottone **Apri file** consente di esaminare il contenuto della richiesta (con particolare riguardo ai dati anagrafici) attraverso lo stesso *viewer* usato per visualizzare i certificati.

4.3.7.3 Generazione CRL

Questa funzione permette di accedere al modulo di generazione di una CRL, i cui dettagli sono descritti nella sezione dedicata.

4.3.7.4 Inizializzazione Dispositivo di Firma

Questa funzione permette di inizializzare una smartcard o altro tipo di dispositivo di firma, nell'ipotesi che tale dispostivo sia del tipo *interfacciato a livello APDU* (si veda la sezione relativa, anche per le istruzioni di configurazione di DigitalSign al fine di riconoscere questi dispositivi). In tali casi, infatti, DigitalSign prende completamente il controllo del dispositivo e vi installa un proprio *file system*, nel quale troveranno posto chiavi, certificati, ecc.

L'operazione di inizializzazione è dunque la prima fase per gestire tali dispositivi; nella memoria del dispositivo vengono collocate alcune informazioni anagrafiche e vengono nel contempo impostate le password (PIN e PUK) per l'accesso al dispositivo stesso.

Come si vede vengono richiesti, nel riquadro più in alto, alcuni dati dall’ovvio significato (viene anche indicata tra parentesi tonde la lunghezza massima di ogni campo in caratteri e viene contrassegnato con un ‘*’ ogni campo di informazione obbligatoria);

Nel riquadro denominato *identificazione* all’utente si richiede l’impostazione di due password:

- la **password d’utente (PIN)** servirà ad effettuare l’operazione di Logon nelle normali attività di utilizzo del dispositivo
- la **password di amministrazione (PUK)** servirà a sbloccare la smartcard nel caso si bloccasse il PIN ed, eventualmente, a de-inizializzare il dispositivo.

Ciascuna delle due password deve essere digitata due volte; per il PIN è possibile anche indicare in numero massimo di tentativi di digitazione errata che il dispositivo deve tollerare prima di andare in blocco, mentre il numero massimo di errori tollerati per il PUK è un dato fisso della smartcard.

Nel campo **Smartcard #** è possibile introdurre un numero di identificazione della smartcard stessa. Se la carta viene fornita da CompEd in genere dispone di un numero di serie stampigliato sull’esterno e si raccomanda di utilizzare qui tale numero, altrimenti si può impostare 0000-0000.

L’utente deve anche decidere in anticipo quanto spazio di memoria (*Storage*) intende riservare per contenere le coppie di chiavi crittografiche.

- Con il bottone **Installa** si opera l’inizializzazione del dispositivo con i dati impostati
- Con il bottone **Annulla** si chiude la finestra senza agire sul dispositivo

4.3.7.5 De-inizializzazione Dispositivo di Firma

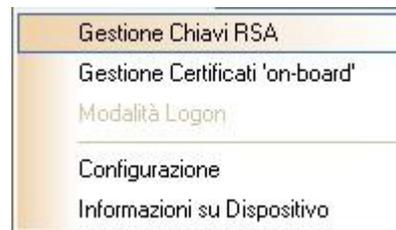
Usando questa funzione su un dispositivo di firma del tipo interfacciato a livello APDU (…) è possibile rimuoverne completamente il contenuto impostato da DigitalSign in fase di Inizializzazione, in generale ripristinandone la “verginità”.

NOTA: questa operazione non è utilizzabile con dispositivi che si trovino in stato di blocco a causa di ripetute digitazioni di PIN o PUK errati.

Per eseguire questa operazione è necessario inserire il PUK:

- Con il bottone Disinstalla si procede alla rimozione dei dati dal dispositivo.
- Con il bottone **Annulla** si chiude la finestra senza agire sul dispositivo.

4.4 Il menu "Dispositivo di Firma"

Questo menu non è disponibile con DigitalSign Reader.
Ogni specifica funzione è in ogni caso abilitata solo se è inserito un dispositivo di firma compatibile con la funzione stessa.

Questo menu raccoglie alcune funzioni di gestione dell'interfacciamento con i dispositivi di firma (smartcard, token USB, ecc.) e dei relativi contenuti.

4.4.1 Gestione Chiavi RSA

Un dispositivo di firma contiene, tra gli altri oggetti, delle coppie di chiavi RSA.
Questa funzione permette di esaminare le chiavi attualmente contenute nel dispositivo, ed eventualmente di intervenire con operazioni di creazione, eliminazione, importazione, esportazione.

I dettagli operativi sono descritti in una sezione dedicata.

4.4.2 Gestione Certificati 'on-board'

Un dispositivo di firma può contenere, tra gli altri oggetti, dei certificati.
Questa funzione permette di accedere al Modulo di Gestione di questi certificati, offrendo in generale opzioni per la visualizzazione e l'esportazione di questi certificati.
Se il particolare dispositivo lo permette è anche possibile caricare certificati nella memoria del dispositivo.

I certificati on-board sono particolarmente importanti perché considerati intrinsecamente attendibili in fase di verifica di firme e certificati.

4.4.3 Modalità Logon

Questa funzione è riservata alla gestione di moduli di controllo di accesso al dispositivo di firma. Principalmente si tratta di una funzione di compatibilità con particolari dispositivi offerti in passato, che potevano attuare l'identificazione dell'utente attraverso un'impronta digitale anziché (oppure in aggiunta al) con il PIN.

Oggi questa funzione è utilizzabile soltanto con dispositivi di firma interfacciati a livello APDU e inizializzati mediante DigitalSign, al fine di sbloccarne il PIN eventualmente bloccato.

NOTA: la funzione non è disponibile con dispositivi interfacciati a livello PKCS#11.

Dapprima viene mostrata la finestra di dialogo qui sopra; agendo sul bottone **Proprietà** l'utente ottiene quest'altra finestra:

I due bottoni disponibili vanno utilizzati secondo la necessità:

- il primo per modificare il PIN esistente (questo bottone è peraltro disabilitato se il dispositivo si trova in stato di blocco):

L'utente deve digitare dapprima il PIN attuale e poi (due volte per scongiurare errori di digitazione) quello nuovo che intende impostare.

- il secondo per sbloccare un dispositivo finito in stato di blocco a causa di ripetute errate digitazioni del PIN:

Qui l'utente deve impostare prima di tutto il PUK e poi (due volte per scongiurare errori di digitazione) il PIN che intende impostare in luogo di quello bloccato.

NOTA: questa funzione può anche essere usata nel caso il PIN non sia ancora bloccato, ma si intenda comunque modificarlo utilizzando il PUK invece del PIN preesistente.

4.4.4 Configurazione

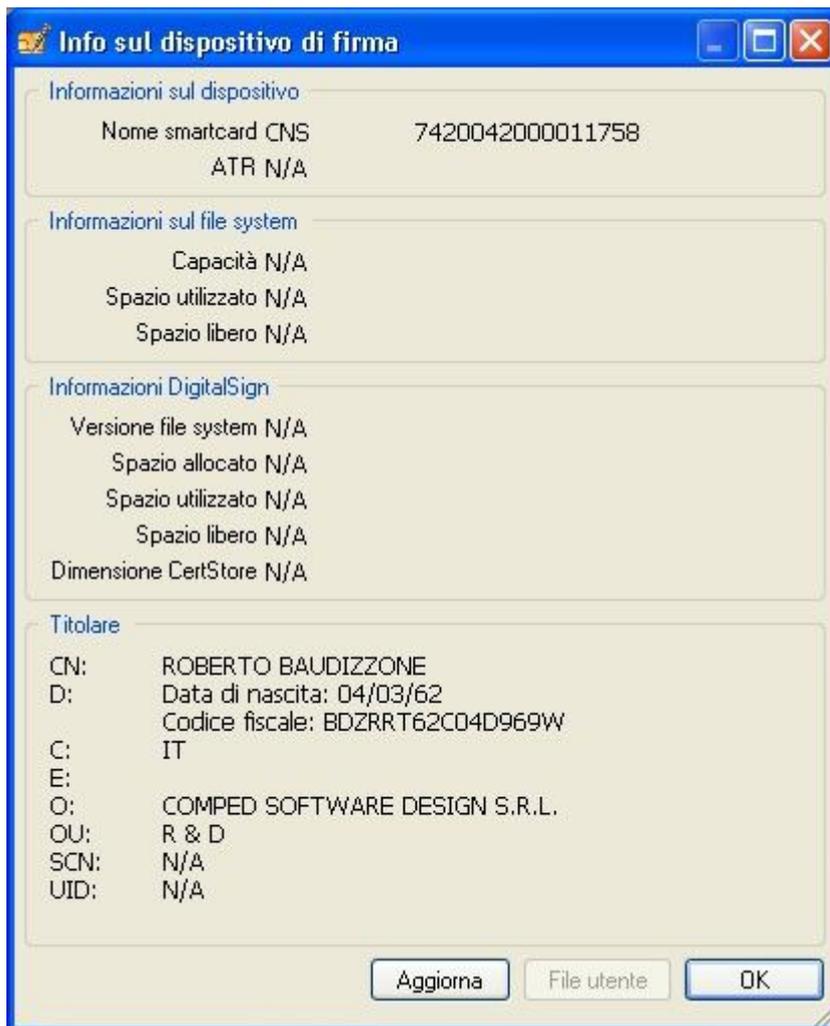
Questa importante funzione serve a controllare la modalità di interfacciamento tra DigitalSign ed il dispositivo di firma.
Per i dettagli si veda la sezione dedicata.

4.4.5 Informazioni sul Dispositivo

Presenta una schermata di informazioni sul dispositivo di firma correntemente inserito.
La visualizzazione è sensibilmente differente secondo che tale dispositivo sia interfacciato a livello APDU oppure in modalità PKCS#11.

- esempio con dispositivo interfacciato a livello APDU, inizializzato da DigitalSign:

In questo caso sono riportate informazioni dettagliate anche sul file system registrato da DigitalSign nella memoria del dispositivo.
È anche disponibile un bottone **File utente** che permette di ispezionare oggetti eventualmente caricati nella memoria del dispositivo da speciali applicazioni.

- esempio con dispositivo PKCS#11 rilasciato da un Certificatore Accreditato:

In questo caso i dati vengono estratti attraverso il *layer* PKCS#11 e non tutti i dati sono disponibili. In particolare mancano tutti i dati sul file system di DigitalSign (che non esiste), mentre i dati del titolare vengono estratti dal certificato qualificato eventualmente reperito nel dispositivo.
Il bottone **File utente** non è abilitato.

In entrambi i casi:
- il bottone **Aggiorna** permette di rileggere i dati dal dispositivo ed aggiornare la visualizzazione
- il bottone **OK** chiude la finestra

4.5 Il menu “Documento”

Questo menu può avere elementi diversi secondo il tipo di documento su cui si sta operando; la figura che segue mostra il caso più completo:

Questo menu è visibile solo quando almeno è presente almeno una finestra documento e di norma contiene uno o più sottomenu.

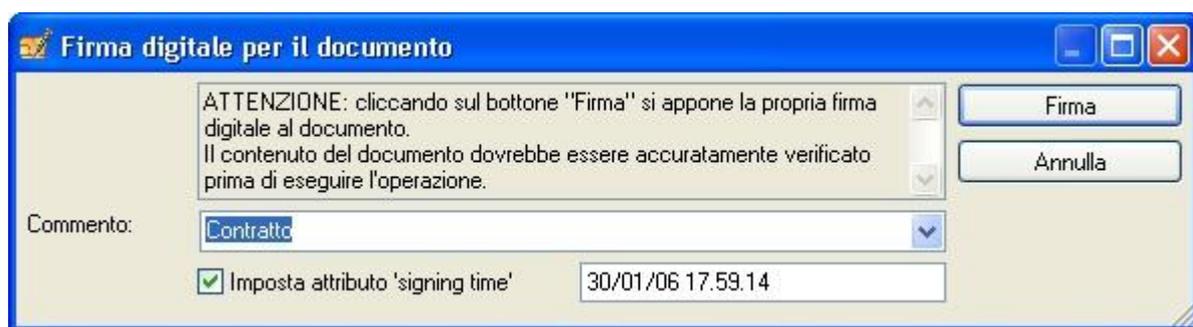
4.5.1 Aggiungi Firma Digitale

Funzione non disponibile con DigitalSign Reader

Consente di firmare digitalmente il documento aperto correntemente selezionato, se è disponibile un dispositivo di firma idoneo e se il documento non contiene ancora una firma digitale corrispondente allo stesso certificato.

NOTA: se viene aperto un documento già corredato di una **Attestazione**, questa funzione è disabilitata. Per evitare ambiguità e per mantenere la conformità ai formati di legge non è consentito mescolare, in uno stesso documento, firme deboli e forti.

Se il documento è già firmato digitalmente l’operazione aggiunge una ulteriore firma di tipo “congiunto”.

Se il dispositivo non è ancora in stato di *Logon* il sistema presenta innanzitutto la finestra di dialogo relativa, quindi quella specifica per la conferma della firma:

Il testo fisso invita l’utente a verificare accuratamente il contenuto del documento, mentre il campo sottostante consente la digitazione di un testo di commento. In effetti questo campo è assistito da una lista, per cui è possibile richiamare i commenti già utilizzati in precedenza.

L’ultima riga di dati permette di controllare l’attributo ***Signing Time*****:** si tratta di un attributo “signed”, ossia coperto dalla firma, che rappresenta la dichiarazione della data ed ora a cui viene apposta la firma (sotto la responsabilità del sottoscrittore, appunto).

L'attributo è opzionale e si imposta attivando il relativo *checkbox*. Il valore effettivo è reimpostato dal sistema con il dato attuale, ma può essere modificato manualmente.

- Con il bottone **Firma** si conferma l'operazione
- Con il bottone **Annulla** si chiude senza generare la firma

4.5.2 Aggiungi Controfirma

Questa funzione è attivabile solo se nel pannello delle proprietà PKCS#7 viene selezionata una firma digitale o una controfirma già esistente, ma generata con un certificato differente da quello attualmente in uso: allora sarà possibile aggiungere una controfirma a tale firma.

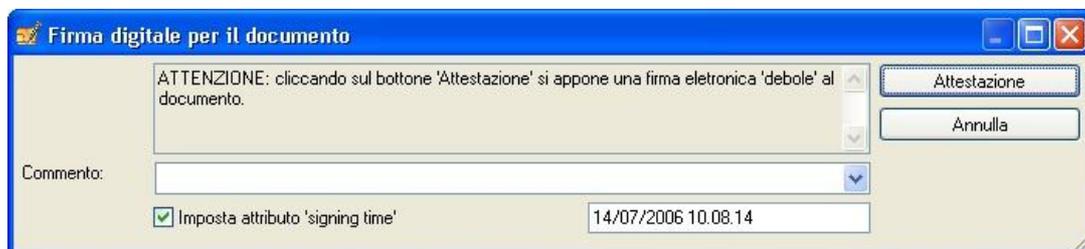
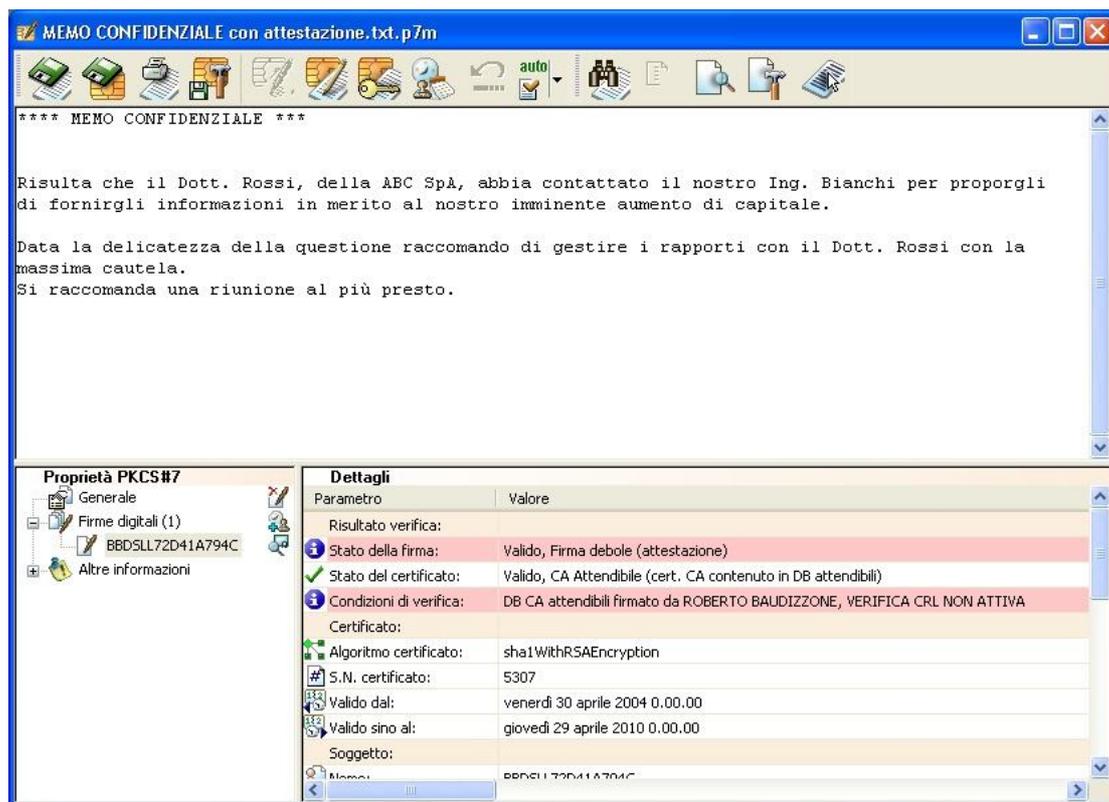
L'operatività è identica a quanto illustrato al punto precedente.

NOTA: la controfirma non è disponibile per le firme deboli o Attestazioni.

4.5.3 Aggiungi Attestazione

Funzione non disponibile con DigitalSign Reader e con DigitalSign Lite; disponibile solo in alcune edizioni, generalizzato solo dopo la versione 3.0.3.37

NOTA: questa funzione è abilitata solo con documenti che ancora non contengono firme di alcun genere, oppure che già contengono una firma debole o Attestazione. Per evitare ambiguità e per mantenere la conformità ai formati di legge non è consentito mescolare, in uno stesso documento, firme deboli e forti.

Il funzionamento di questa opzione è del tutto analogo a quello di aggiunta di una firma digitale. La finestra di conferma è leggermente diversa:

Il risultato dell'apposizione di una attestazione è del tutto analogo, ma il riquadro proprietà della firma mostra chiaramente che si tratta di una firma particolare:

NOTA: la figura qui sopra fornisce anche un interessante esempio di come DigitalSign visualizza il risultato della verifica: una linea colorata evidenza che non si tratta di una firma digitale apposta con un certificato qualificato, bensì di una Attestazione o firma debole; quanto alla verifica del certificato esso è considerato attendibile per mezzo del DB attendibile (si veda la sezione relativa alla configurazione dell'attendibilità), dichiarato tale da chi lo ha firmato.
Viene anche evidenziato che in questo momento non è in funzione la verifica dello stato di revoca.
Per i dettagli sulle differenze concettuali tra una Firma Digitale a pieno valore legale ed una Attestazione si veda la sezione relativa.

4.5.4 Marca Temporale

Funzione non disponibile con DigitalSign Reader e con DigitalSign Lite

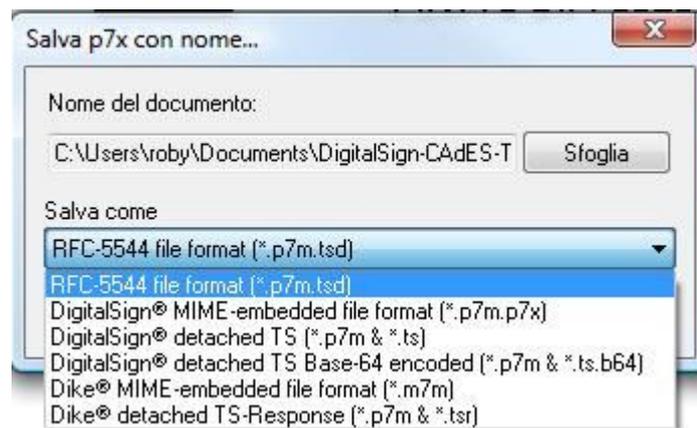
Permette di associare una marca temporale ad un documento.

Il sistema presenta questa finestra di dialogo, per chiedere conferma all'utente.

DigitalSign può operare con diversi account di marcatura temporale, da configurare opportunamente tramite il bottone **Configurazione** (equivalente al menu **Strumenti -> Configurazione Servizi**), giungendo al modulo di configurazione specifico.

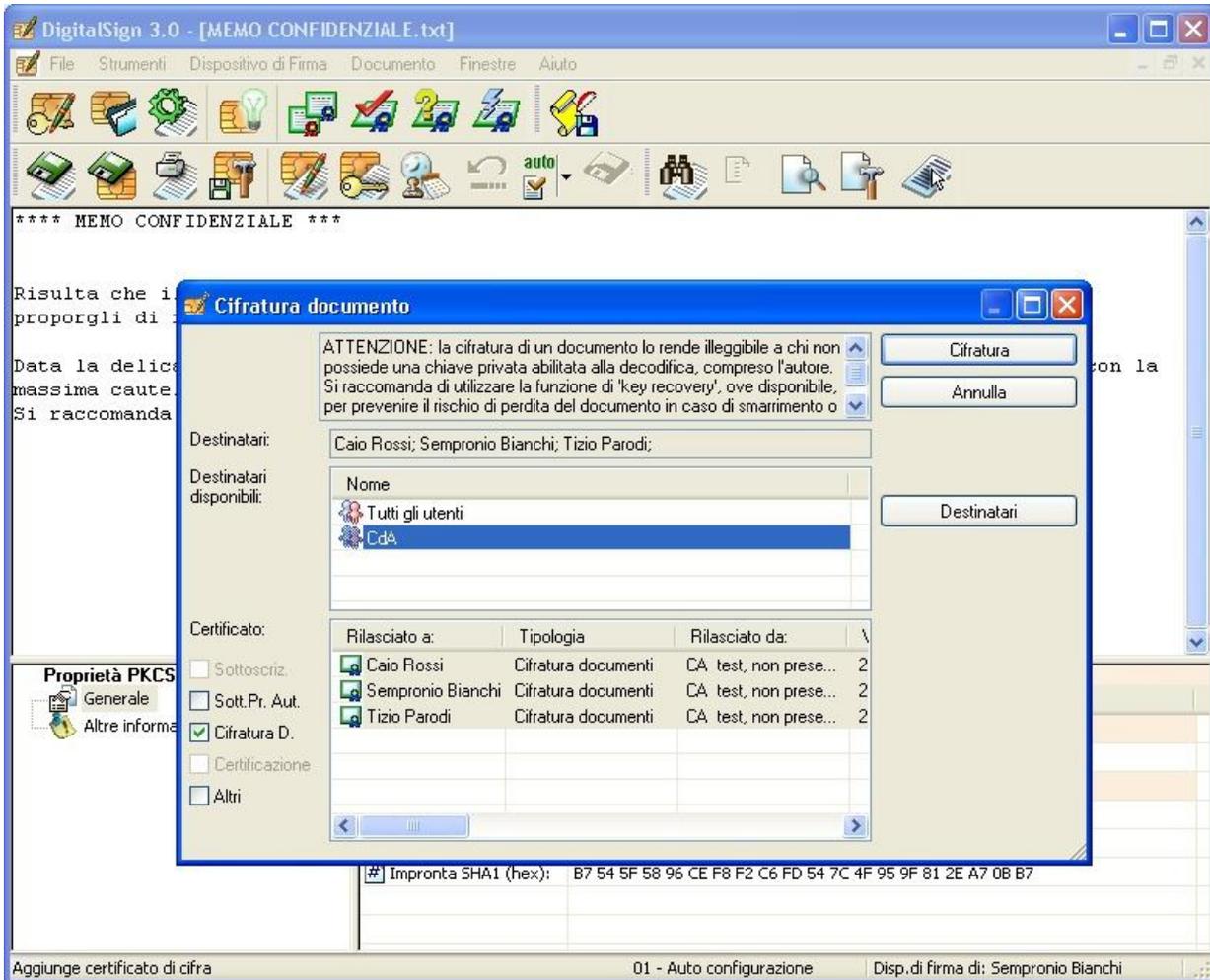
La *listbox* della finestra mostra l'account qualificato come predefinito, ma consente, nel caso vi siano più account configurati, di scegliere quale impiegare.

– Il bottone **Configurazione** conduce al modulo di configurazione degli account di marcatura temporale
– Il bottone **Applica timestamp** esegue l'operazione, collegandosi al server della TSA ed ottenendo la marca temporale associata al documento su cui si sta operando
– Il bottone **Annulla** chiude l'operazione senza richiedere la marca temporale alla TSA.

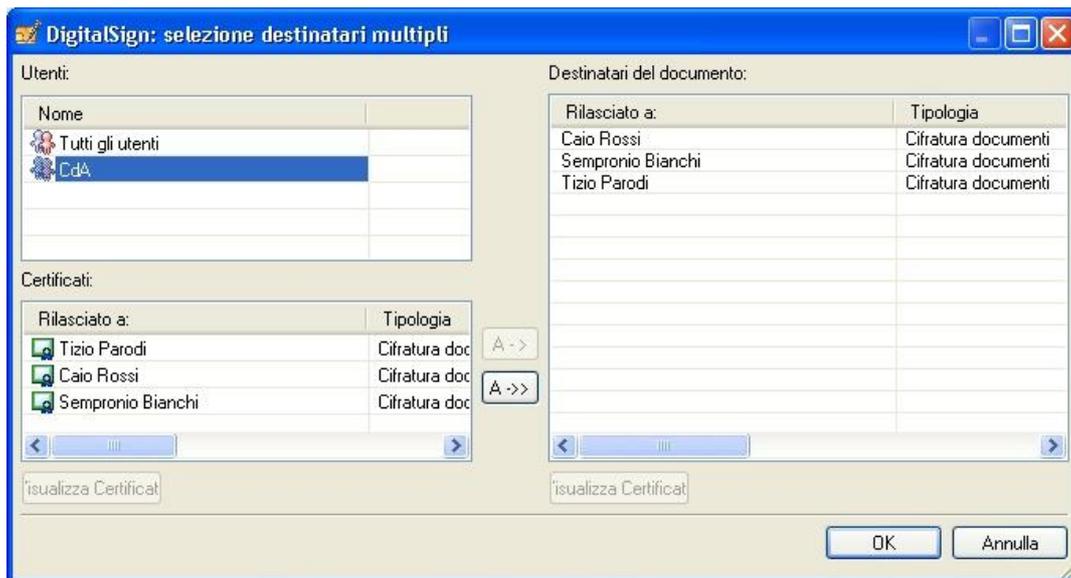
Si noti che subito dopo aver eseguito l'operazione di applicazione del timestamp la marca temporale viene mantenuta solo in memoria.
Soltanto al momento in cui l'utente disporrà il salvataggio su disco (con **File -> Salva Documento** o **Salva Documento con nome…**) verrà richiesto all'utente di scegliere una modalità di rappresentazione tra quelle supportate da DigitalSign.

4.5.5 Destinatario Cifratura

Funzione non disponibile con DigitalSign Reader e con DigitalSign Lite

Permette di cifrare il contenuto del documento correntemente aperto a beneficio di uno o più destinatari.
Per i dettagli sulle modalità attuate da DigitalSign per cifrare i dati si veda la sezione relativa.
Si tenga comunque presente che la cifratura attuata da DigitalSign è in prima approssimazione di tipo "asimmetrico": si cifra utilizzando la chiave pubblica del soggetto abilitato a leggere i dati, in modo che quest'ultimo possa leggerli usando la corrispondente chiave privata a sua esclusiva disposizione.
In effetti è possibile cifrare a beneficio di molteplici soggetti, che vengono definiti "destinatari".
DigitalSign include sempre nella lista di questi destinatari lo stesso autore del messaggio, in modo che esso possa sempre leggere il contenuto del documento. A tale scopo DigitalSign richiede che, al momento in cui si richiede la cifratura di un documento aperto, sia inserita una smartcard, così da leggere il certificato da impiegare e da disporre della chiave privata necessaria alla rivisualizzazione una volta eseguita la codifica.

Ecco cosa appare sullo schermo appena si attiva il comando:

La schermata presenta una lista suddivisa in due riquadri, il primo dei quali mostra tutti i Gruppi di destinatari definiti (incluso il gruppo speciale **Tutti gli utenti**). Il secondo riquadro mostra tutti i certificati appartenente al Gruppo selezionato.
La definizione dei Gruppi (disponibile solo a partire dalla versione 3.0.3.35) si effettua dal modulo di gestione del DB locale dei certificati.

L'utente può posizionarsi sul riquadro inferiore e scegliere uno specifico singolo destinatario, oppure posizionarsi sul riquadro superiore e scegliere un intero Gruppo (escluso Tutti gli utenti): agendo sul bottone **Cifratura** per chiudere la finestra con la selezione effettuata.

Oppure l'utente può desiderare una selezione più articolata di destinatari, magari includendo più gruppi ed alcuni soggetti singoli, agendo sul bottone **Destinatari**, che conduce a questa schermata:

Il riquadro in alto a sinistra elenca i Gruppi disponibili; il riquadro sottostante mostra i certificati contenuti nel Gruppo selezionato.
Si opera selezionando un Gruppo nel primo riquadro oppure un destinatario singolo nel secondo riquadro, quindi premendo il bottone **[A ->]** oppure **[A ->>]** per includere il singolo destinatario o l'intero gruppo, rispettivamente, nella lista finale.
Nel riquadro di destra è sempre possibile selezionare un destinatario ed eliminarlo dalla lista con il tasto **[Canc]**.

- Con il bottone **Annulla**, naturalmente, si esce senza aggiornare la lista.
- Con i bottoni **Visualizza Certificato** è possibile ispezionare i certificati dei riquadri corrispondenti.

Dopo aver cifrato un documento l'utente può desiderare di cancellare dal proprio sistema la versione originale (non cifrata) del documento. Questo è possibile con la funzione Wipe File.

NOTA: le versioni di DigitalSign precedenti alla 3.0.3.35 non dispongono della gestione dei Gruppi e consentono di selezionare solo un singolo certificato alla volta.

NOTA IMPORTANTE: per facilitare l'utilizzo della cifratura anche con certificati autoprodotti DigitalSign non richiede che i relativi certificati siano verificati in termini di attendibilità del Certificatore che li ha emessi. Tuttavia l'utente dovrebbe assicurarsi dell'autenticità del certificato di un destinatario, specie se tale certificato corrisponde ad un soggetto non conosciuto personalmente o se è stato ricevuto via email.
Le funzioni di visualizzazione del certificato, in ogni contesto, consentono di effettuare la verifica.

NOTA IMPORTANTE: qualora si utilizzino le funzionalità di cifratura per rendere riservati i propri documenti si tenga sempre presente che l'apertura dei documenti cifrati richiede la disponibilità della chiave privata.
È dunque quanto mai raccomandato effettuare copie *(key recovery)* delle proprie chiavi private di cifratura, in modo da poterle ripristinare in caso di danneggiamento o perdita della smartcard.
Per le modalità di esportazione di queste chiavi si veda la sezione relativa alla gestione delle coppie di chiavi.

4.5.6 Annulla Tutto

Questo comando, ove applicabile, consente di annullare le modifiche fin qui apportate al documento aperto, ripristinandone lo stato preesistente.

4.5.7 Wipe File

Funzione non disponibile con DigitalSign Reader e con DigitalSign Lite; introdotta solo a partire dalla versione 3.0.3.37

Questo comando viene abilitato solo dopo che si realizza la cifratura di un documento e dopo il salvataggio del documento cifrato risultante.
La funzione “*wipe*” consiste nella cancellazione del file originale (in chiaro) ed avviene solo dietro esplicita conferma dell’utente.
DigitalSign, con questa funzione, non si limita a cancellare il file, ma mette in atto alcune misure volte ad aumentare la sicurezza dell’operazione, nel senso di eliminare ogni traccia del documento non cifrato dal file system dell’utente:

1. il file viene sovrascritto per tre volte con dati casuali (per eliminare tracce dei dati originali);
2. il file viene rinominato per tre volte (per eliminare tracce del nome originale);
3. il file viene impostato a lunghezza pari a zero (per rimuovere il collegamento con i settori del dico che ospitavano i dati);
4. il file viene effettivamente cancellato a livello del sistema operativo.

NOTA IMPORTANTE: quantunque le misure descritte rappresentino quanto di meglio DigitalSign possa fare per evitare che i dati in chiaro siano recuperabili dal sistema, esistono dei limiti oggettivi sull’efficacia di tali misure:

a) se il documento originale era stato predisposto con una applicazione di tipo “office”, come per esempio MS Word oppure Excel, tale applicazione probablmente manterrà – almeno durante la redazione del documento – uno o più file temporanei che potrebbero contenere tracce dei dati. Al termine dell’esecuzione, in generale, queste applicazioni cancellano i propri file temporanei con semplici comandi di cancellazione a livello del sistema operativo. DigitalSign, evidentemente, non può nulla per evitare il recupero dei dati da questi file;
b) quando il sistema operativo adotta un file system come NTFS esso ha la possibilità di spostare autonomamente i dati di un file da una parte all’altra del disco, di fatto eseguendo delle copie dei dati. In questi casi la cancellazione accurata dei dati dall’ultima copia del file nulla può contro la ricuperabilità dei dati dalle copie preesistenti

Per quanto sopra l’utente particolarmente sensibile al problema dell’eliminazione dei propri dati sensibili dopo la cifratura di un documento dovrebbe ricorrere ad altri strumenti specializzati, che provvedano alla sovrascrittura sistematica di tutti i settori del disco dichiarati “spazio libero” dal sistema operativo.

Da ultimo è appena il caso di notare che la cancellazione della copia originale di un documento cifrato va effettuata con cautela: nel caso venisse perduta la chiave privata abilitata a decifrare il documento non esisterà più alcun modo per recuperarne il contenuto.

4.5.8 Verifica alla data

Questo comando consente di impostare una data ed ora di riferimento, diversa dall’istante presente, per la verifica delle firme digitali del documento corrente.
Si rimanda per i dettagli all’apposita sezione

4.5.9 Sottomenu Modalità Visualizzazione

Questo comando conduce ad un sottomenu contenente le varie modalità di visualizzazione supportate.

Di regola la modalità selezionata è quella Automatica, che permette a DigitalSign di utilizzare automaticamente la modalità idonea a presentare il documento.
Nel menu è anche riportata in grassetto la modalità effettiva attualmente utilizzata.

Nel caso l'utente ritenesse di utilizzare una modalità diversa (per esempio quella esadecimale) può operare la propria scelta in questo menu.

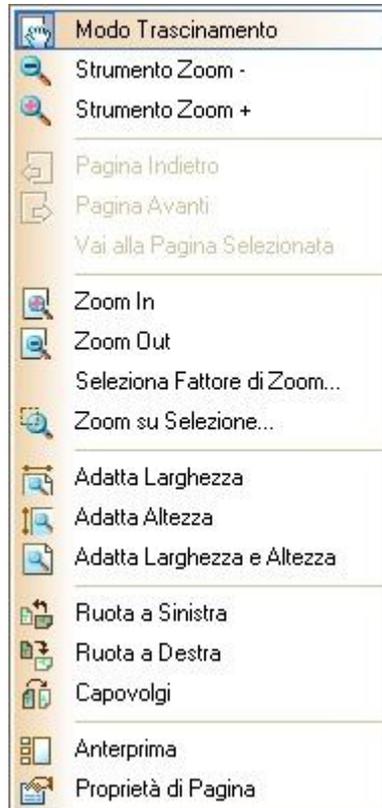
4.5.10 Sottomenu Securview ASCIII/RTF

Questo sottomenu del menu Documento è disponibile quando si opera su un documento di tipo testo oppure Rich Text Format.

Le sue funzioni sono molto intuitive e comprendono:

- **Ricerca**
  Permette di ricercare una sottostringa nel testo
- **Copia**
  Previa selezione di una porzione di testo, permette di copiarla negli appunti
- **Seleziona tutto**
  Dopo l'attivazione di questa funzione, con Copia si passa tutto il testo negli appunti
- **Imposta pagina**
  Apre una finestra di dialogo per impostare le opzioni di stampa
- **Anteprima di stampa**
  Apre la tipica funzione di anteprima di stampa per il documento

4.5.11 Sottomenu Securview Imaging

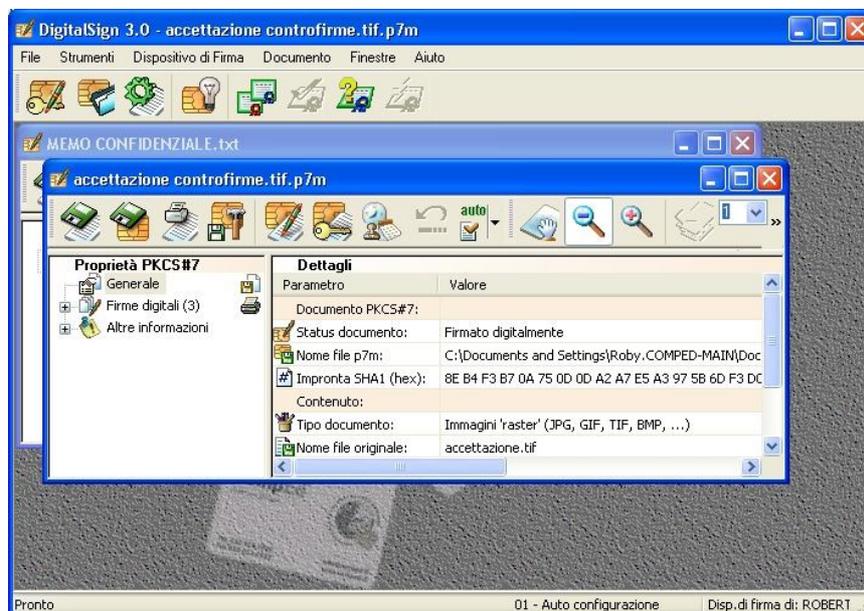
Questo sottomenu del menu Documento è disponibile quando si opera su un'immagine o un documento sostituito da grafica raster.

- **Modo Trascinamento**
  Il puntatore del mouse può essere usato (tenendo premuto il tasto sinistro) per spostare l'immagine nel riquadro di visualizzazione
- **Strumento Zoom – e Zoom +**
  Il puntatore del mouse può essere usato, mediante un click, per ridurre od aumentare il fattore di ingrandimento
- **Pagina indietro, Avanti, Selezionata**
  Queste funzioni sono abilitate solo se si opera su documenti in formato multipagina (es. TIFF) e permettono di navigare attraverso le pagine
- **Zoom In e Zoom Out**
  Simili agli strumenti corrispondenti, modificano immediatamente il fattore di ingrandimento
- **Selezione Fattore di Zoom**
  Permette di digitare direttamente il fattore di zoom desiderato
- **Zoom su selezione**
  Permette di selezionare liberamente un'area ristretta dell'immagine; rilasciando il tasto del mouse l'ingrandimento viene immediatamente modificato per ingrandire l'area selezionata
- **Adatta Larghezza, Altezza, Larghezza ed Altezza**
  Modifica l'ingrandimento in modo da rendere visibile tutta la larghezza, oppure tutta l'altezza, oppure tutta l'immagine
- **Ruota a Sinistra, a Destra, Capovolgi**
  Modifica l'orientamento dell'immagine visualizzata

- **Anteprima, Proprietà di pagina**
  Permette di configurare e controllare la stampa

4.6 Il menu "Finestre"

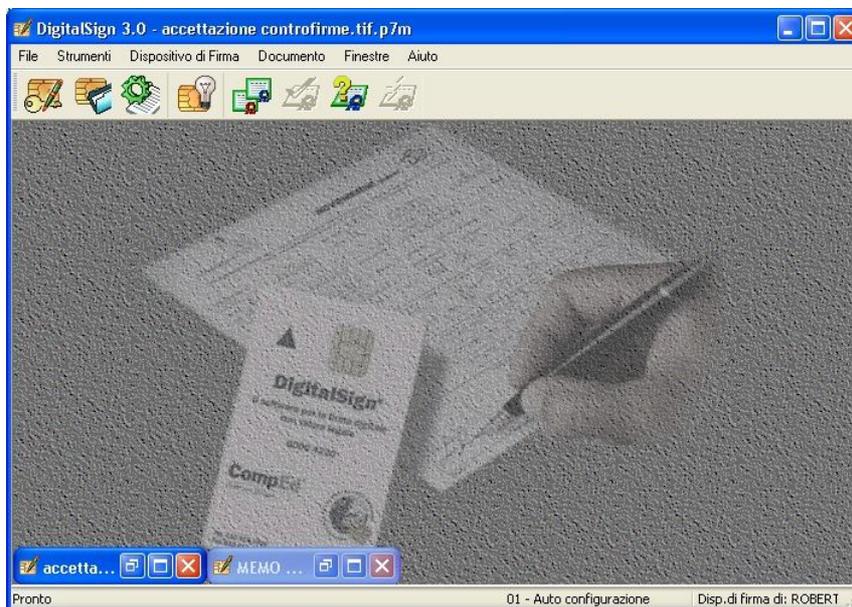
Questo menu fornisce alcuni comandi standard per riorganizzare la visualizzazione delle diverse finestre controllate da DigitalSign.
Se sono aperte una o più finestre documento le ultime voci del menu corrispondono a tali finestre, consentendo di riportare in primo piano tali finestre.

4.6.1 Sovrapponi

Rivisualizza le finestre documento eventualmente aperte in DigitalSign nella classica modalità sovrapposta, in modo che siano visibili i titoli di tutte le finestre (rendendo quindi agevole il passaggio da una all'altra) e che una di esse sia in primo piano.

4.6.2 Affianca

Rivisualizza le finestre documento eventualmente aperte in DigitalSign nella classica modalità affiancata, in modo che tutte le finestre siano visibili, per quanto in porzione ridotta, una sotto l'altra.

4.6.3 Disponi Icone

Questo comando ha effetto sulle finestre che eventualmente si trovassero nello stato iconizzato: le icone vengono disposte in modo ordinato alla base della finestra principale.

4.6.4 Mostra pannelli di informazione

Attiva o disattiva la visualizzazione dei pannelli informativi decritti nella sezione dedicata

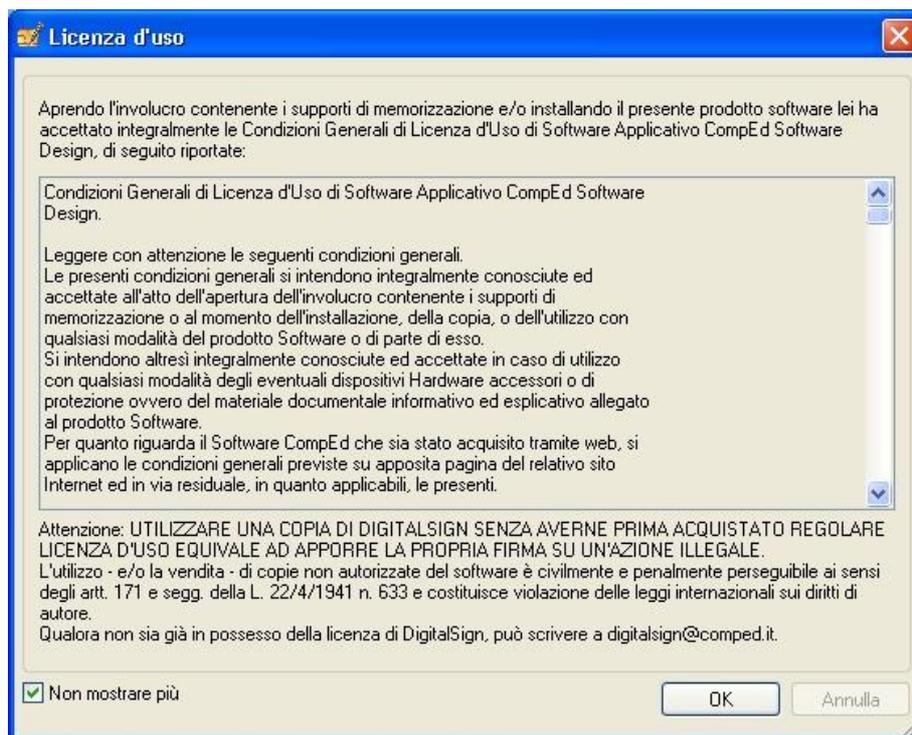
4.7 Il menu "Aiuto"

Questo menu offre alcune funzioni per visualizzare informazioni generali sulla versione del software in proprio possesso, sulla licenza d’uso, per registrare o attivare la propria copia del software.

4.7.1 Documentazione

Questa funzione provoca la visualizzazione della presente documentazione, se questa è disponibile e se la macchina dispone del software necessario alla visualizzazione (un viewer per il formato PDF).

4.7.2 Mostra Licenza d’uso

Visualizza la stessa schermata con le condizioni di licenza d’uso che viene normalmente visualizzata al primo avvio dell’applicazione.

La schermata viene mostrata ad ogni avvio, a meno che l’utente non selezioni il checkbox **Non mostrare più**.
Questo comando nel menu **Aiuto** serve proprio a rivisualizzare il testo in questo caso ed eventualmente modificare l’istruzione di evitare le prossime visualizzazioni.

4.7.3 Procedura di Registrazione

La procedura di Registrazione è obbligatoria su alcune edizioni di DigitalSign (Reader, Lite, Professional Integrated) mentre può essere opzionale in altre (Professional) o addirittura non prevista (edizioni Professional OEM).
Alcuni distributori possono fornire licenze di DigitalSign pre-registrate o che sostituiscono la procedura di registrazione con un collegamento ad un sistema centralizzato di controllo delle licenze.

Questo comando, se applicabile, provoca l'esecuzione della procedura di Registrazione del prodotto.
Tale procedura, per le edizioni ed i casi previsti, viene di norma eseguita automaticamente al primo avvio dell'applicazione.

4.7.4 Attivazione

La procedura di attivazione segue quella di Registrazione e consiste nell'inserimento di un Codice di Attivazione fornito dal sistema di registrazione di CompEd.
Di norma questa funzione viene eseguita automaticamente di seguito a quella di Registrazione, ma esistono alcuni casi in cui l'utente può avere la necessità di avviare la procedura autonomamente, tramite questa funzione del menu.

4.7.5 Informazioni su DigitalSign

Presenta una schermata di questo tipo:

NOTA: In alcune edizioni OEM (personalizzate per grandi clienti) la visualizzazione può essere diversa e contenere il logo dell'organizzazione.

Da questa immagine l'utente può ricavare le indicazioni esatte sull'edizione e sul numero di versione della propria copia di DigitalSign, nonché sull'identità dell'utente registrato.

È anche presente un link per accedere ad una pagina di *“credits”* per **OpenSSL**: si tratta di una libreria crittografica *Open Source* il cui utilizzo (da parte di CompEd, come da parte di migliaia di operatori nel mondo) è condizionato al fatto che siano visibili da parte dell’utente le informazioni riportate a seguito dell’azionamento di tale link.

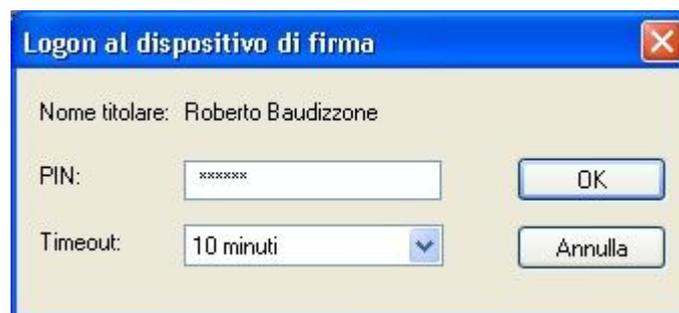
È presente anche un link alla pagina principale del sito di CompEd.

Il bottone **Info Registrazione**, se presente, apre una piccola finestra di dialogo contenente, a scopo di riferimento, le principali informazioni relative alla registrazione/attivazione del prodotto:

4.8 Moduli di gestione e finestre di dialogo

In questa sezione sono raccolte le descrizioni di alcuni moduli funzionali di DigitalSign utilizzati in diversi contesti.

4.8.1 Logon al dispositivo di firma

Questa finestra di dialogo viene presentata all’utente al momento in cui è richiesto che esso si identifichi – introducendo il PIN che solo il titolare deve conoscere – come legittimo titolare del dispositivo di firma correntemente in uso.

La finestra viene presentata quando l’utente richiede esplicitamente di effettuare il logon (dal menu **File**) oppure quando viene avviata un’operazione che coinvolge oggetti contenuti nell’area privata del dispositivo stesso, il quale si trova in stato di Logoff.

Nel campo **PIN** si digita appunto il codice di identificazione, che viene visualizzato in modo mascherato per impedire che venga carpito da chi osserva da dietro le spalle dell’utente.

Il campo **Timeout** corrisponde ad una *listbox* che permette di scegliere un periodo di tempo, da 1 minuto sino a 10 minuti, oppure ‘nessuno’. Si tratta del tempo massimo per cui il dispositivo

permane in stato di Logon senza che si verifichi alcuna attività con il dispositivo stesso.
Se si seleziona 'nessuno' il dispositivo non andrà in Logoff sino all'esplicito comando, oppure sino a che l'utente non rimuove il dispositivo o chiude l'applicazione.

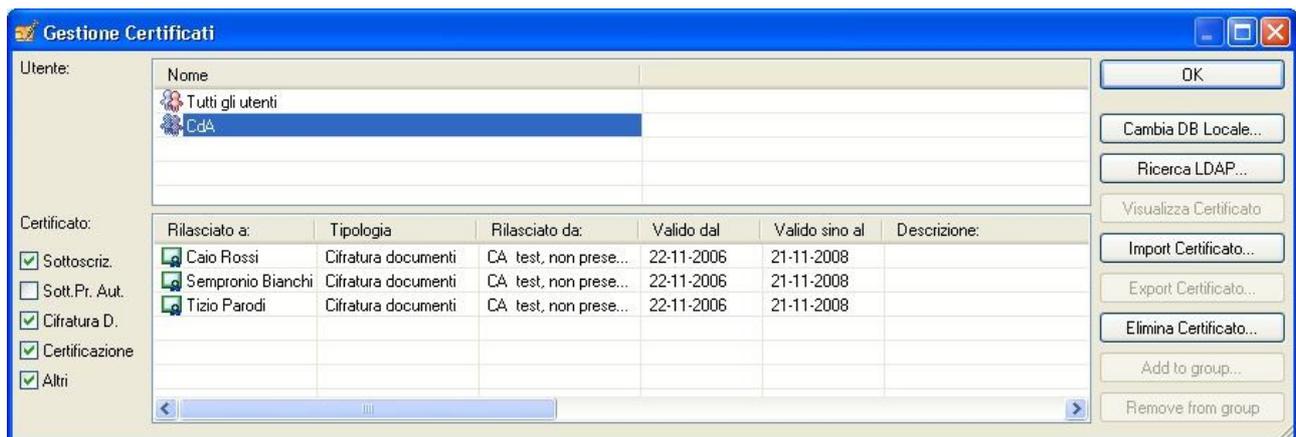
- Con il bottone **OK** si conferma il dato digitato.
- Con il bottone **Annulla** si esce senza inviare il codice al dispositivo di firma.

4.8.2 Modulo di gestione del DB dei Certificati

Il DB locale dei certificati è un archivio destinato, appunto, a contenere certificati.
Questo archivio può servire a diversi scopi, secondo che si operi in modalità di security **STRONG** oppure **SOFT** (si veda la sezione relativa).

- in modalità **STRONG** DigitalSign basa le verifiche dei certificati su una lista di CA dichiarate accreditate e/o attendibili tramite la firma del Presidente di CNIPA oltre che – opzionalmente – tramite la firma di un ulteriore soggetto che si assume la responsabilità di dichiarare attendibili altre CA non accreditate.
  Quindi il DB locale non serve a contenere certificati di riferimento per le operazioni di verifica, ma di fatto funge solo da "rubrica" di certificati da utilizzare per le operazioni di crittografia.
  Come illustrato a proposito della cifratura dei documenti, l'utente che si accinge a codificare un contenuto sceglierà da questo archivio il soggetto o i soggetti abilitati a decifrarlo;
- in modalità **SOFT** DigitalSign verifica positivamente i certificati emessi da qualunque CA il cui certificato si trovi nel DB locale, quindi il DB locale serve proprio a contenere i certificati delle CA considerate attendibili.

IL DB locale dei certificati rappresenta anche l'archivio "naturale" dei certificati emessi con la **Personal Certification Authority**.

Il modulo di gestione si presenta come nella seguente figura:

Il riquadro superiore contiene l'elenco dei **Gruppi** correntemente definiti: per default è sempre definito il gruppo speciale "Tutti gli utenti".

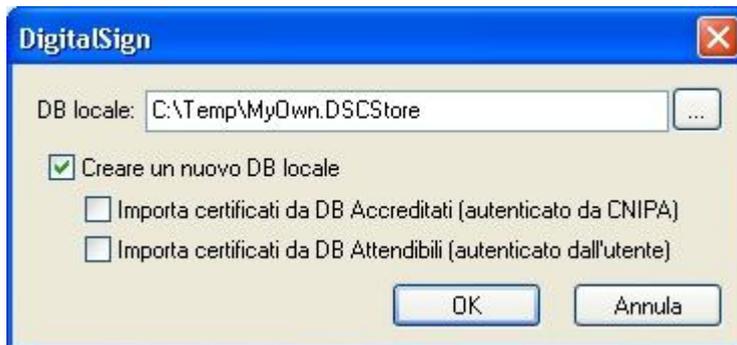
NOTA: il comportamento di DigitalSign a questo riguardo è cambiato a partire dalla versione 3.0.3.35: le versioni precedenti, infatti, non supportavano i Gruppi e visualizzavano nella parte alta della finestra l'intero insieme dei titolari di certificato.

Il riquadro inferiore contiene una lista dei certificati contenuti nel Gruppo correntemente selezionato nella finestra superiore; se nel riquadro superiore è selezionato il Gruppo **Tutti gli utenti** allora il riquadro inferiore mostra tutti i certificati dell'archivio.

NOTA: il comportamento di DigitalSign a questo riguardo è cambiato a partire dalla versione 3.0.3.35: nelle versioni precedenti il riquadro inferiore presentava i certificati intestati al singolo soggetto correntemente selezionato nel riquadro superiore.

Si noti che diversi certificati rilasciati ad uno stesso soggetto da diverse Certification Authority possono scriverne il nominativo in modo differente, facendo sì che in questa finestra tale soggetto appaia come due o più soggetti diversi.

Sulla sinistra compare una batteria di *checkbox* che permette di abilitare o disabilitare la visualizzazione di diverse tipologie di certificato.

– Con il bottone **OK** si chiude la finestra
– Con il bottone **Cambia DB Locale** è possibile mettere in uso un diverso DB.
  Compare in tal caso una finestra di questo tipo:

  È possibile selezionare un diverso file, sfogliando con il bottone **[...]**, oppure crearne uno nuovo – vuoto – impostando il nome e selezionando l'apposito *checkbox*.
  Altri due *checkbox* permettono di pre-caricare nel nuovo DB tutti i certificati del DB autenticato da CNIPA e di quello dichiarato attendibile dall'utente (operazione utile per esperimenti di verifica).
– Con il bottone **Ricerca LDAP** è possibile accedere al server LDAP gestito da un certificatore e ricercare certificati. La lista dei server disponibili per questa ricerca si gestisce attraverso il menu Strumenti -> Configurazione Servizi -> Elenchi in linea LDAP.
– Con **Visualizza Certificato** si apre la finestra di visualizzazione del certificato selezionato.
– Con **Import Certificato** è possibile importare nel DB un certificato disponibile su file.
– Con **Export Certificato** è possibile esportare su file il certificato correntemente selezionato
– Con **Elimina certificato** si rimuove dal DB il certificato selezionato
– Con **Aggiungi a Gruppo** è possibile includere il certificato correntemente selezionato in un particolare Gruppo, eventualmente creato appositamente.
  Scopo principale dei Gruppi è predefinire delle "liste di destinatari" da utilizzare frequentemente per le operazioni di cifratura dei contenuti.

Si apre una ulteriore finestra di dialogo:

La finestra mostra i Gruppi già definiti (eventualmente vuota); se il gruppo a cui si intende aggiungere il certificato selezionato è già esistente è sufficiente fare click sulla casella corrispondente. Altrimenti è possibile creare subito un Nuovo Gruppo con il bottone corrispondente.

NOTA: questo comando non esiste nelle versioni precedenti la 3.0.3.35

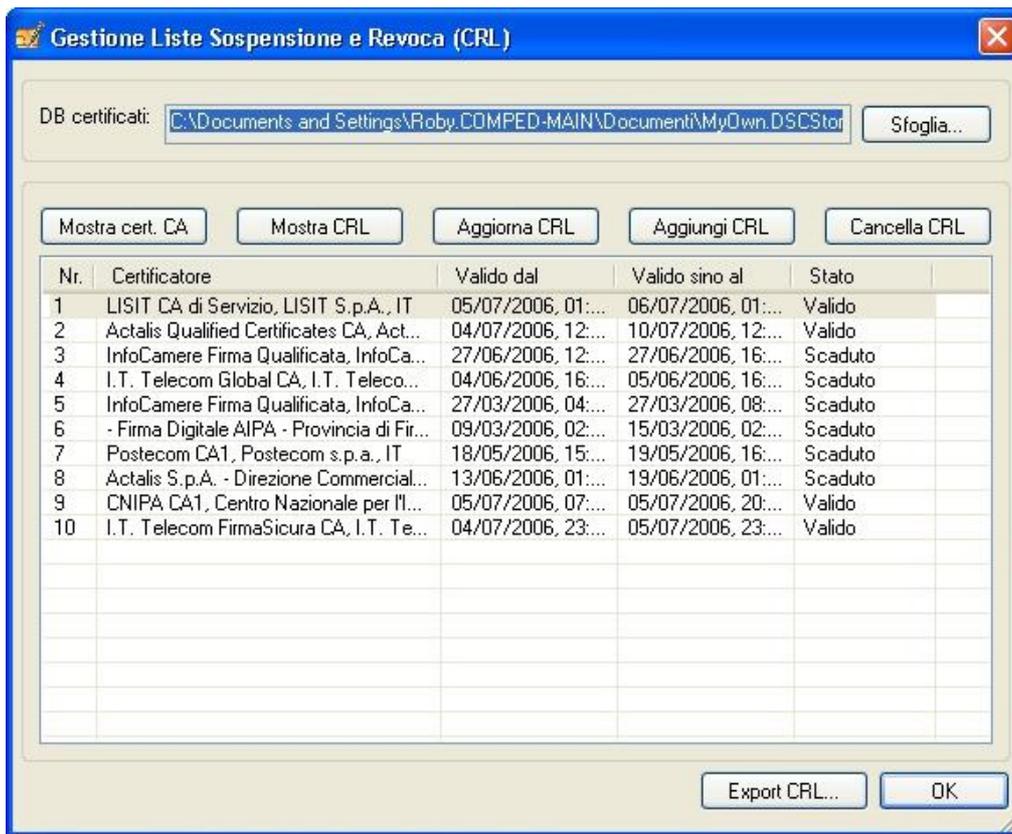
– Con **Rimuovi dal Gruppo** è possibile far sì che il certificato correntemente selezionato nel riquadro inferiore (e quindi appartenente al Gruppo selezionato nel riquadro superiore) venga eliminato dal gruppo stesso.

  NOTA: questo comando non esiste nelle versioni precedenti la 3.0.3.35

4.8.3 Modulo di Gestione delle Liste di Sospensione e Revoca (CRL)

Man mano che DigitalSign esegue operazioni di verifica di certificati, se è attiva la funzione di verifica dello stato di sospensione e revoca, accede ai server delle CA che hanno emesso i certificati e scarica le relative CRL (Liste di Sospensione e Revoca).
Si ricorda che l'indirizzo URL a cui si reperisce una CRL è scritto nel certificato stesso, nell'estensione standard CDP (CRL Distribution Point), protetta dalla firma del Certificatore stesso.

Ogni CRL scaricata viene automaticamente memorizzata all'interno dello stesso file che ospita anche il DB locale, sovrascrivendo l'eventuale copia più vecchia della stessa lista.

Il modulo di gestione delle CRL si presenta come in figura:

La lista presenta tutte le CRL disponibili, con una organizzazione in colonne:

- **Certificatore**: il nominativo del certificatore che ha emesso la lista
- **Valido dal**: la data ed ora di inizio validità della lista. Coincide con la data ed ora di emissione da parte del certificatore ed è un dato coperto dalla firma digitale del Certificatore stesso
- **Valido sino al:** rappresenta il temine di validità della CRL, che dovrebbe coincidere con la pubblicazione del prossimo aggiornamento della CRL da parte del certificatore
- **Stato:** valido o non valido, in base al momento attuale ed alla finestra di validità dichiarata con i due campi "Valido dal" e "Valido sino al"

In alto compare il nome (completo di percorso) del file contenente le CRL sotto osservazione. Con il bottone **Sfoglia** è possibile esplorare altri file, che devono comunque essere del tipo "DB locale".

– con il bottone **Mostra certificato di CA** si ottiene la visualizzazione del certificato della Certification Authority che ha emesso la CRL selezionata, tramite l'apposito viewer
– Con il bottone **Mostra CRL** si visualizza il contenuto della CRL correntemente selezionata, mediante un viewer specifico
– Con il bottone **Aggiorna CRL** si provoca l'immediata rilettura della CRL aggiornata dal server della CA. Si noti che questa funzione non è utilizzabile con tutte le CA: può funzionare solo nel caso in cui il certificato della CA contenga l'estensione CDP (CRL Distribution Point) e che alla URL così ottenuta sia presente la CRL corrispondente
– Con **Aggiungi CRL** è possibile caricare nell'archivio una CRL disponibile su un file, ottenuta con altri mezzi
– Con **Cancella CRL** si può eliminare dall'archivio la CRL selezionata.

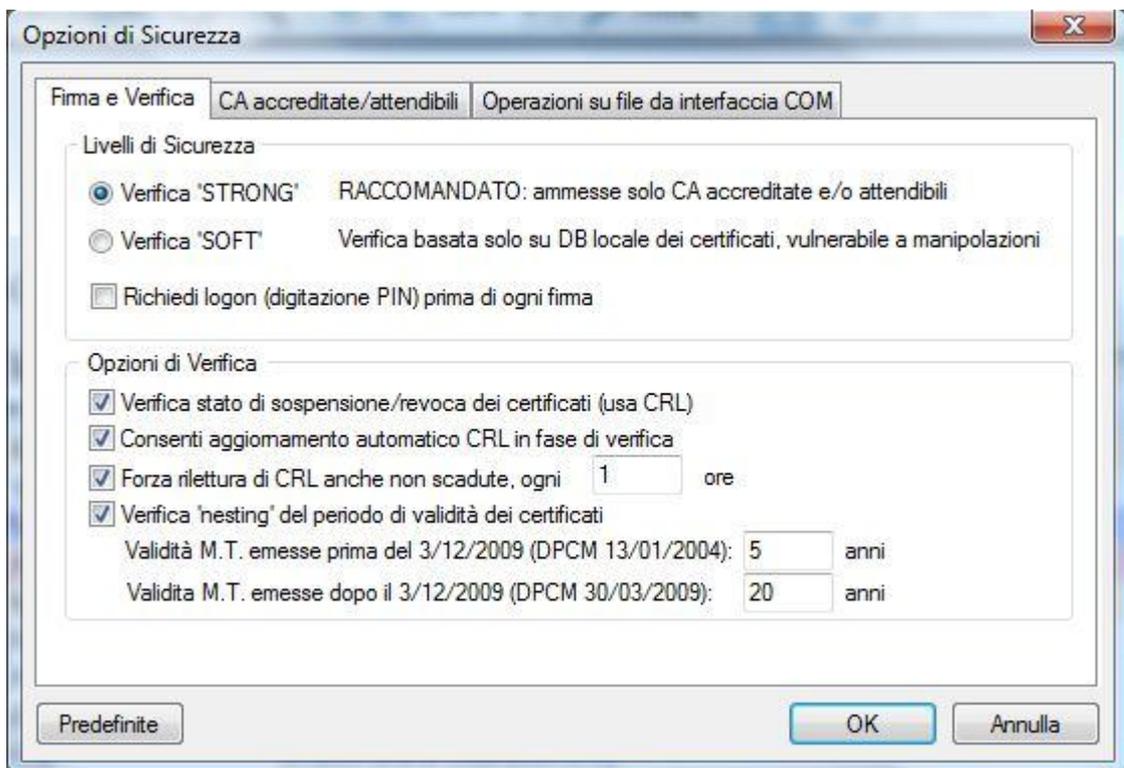
- Con **Export CRL** è possibile esportare su un file la CRL selezionata
- Con il bottone **OK** si chiude la finestra

Per informazioni sulle strategie attuate da DigitalSign nell'utilizzo delle CRL per la verifica di firme e certificati si veda la sezione relativa.

4.8.4 Modulo di Gestione delle Opzioni di Security

Questo modulo di configurazione presenta tre diverse cartelle per gestire altrettante serie di parametri.
Per tutte le cartelle sono disponibili i seguenti bottoni:

- **Predefinite** – ripristina i valori di default
- **OK** – salva le modifiche e chiude la finestra
- **Annulla** – chiude la finestra senza salvare le modifiche eventualmente apportate

4.8.4.1 Firma e verifica

Questo pannello consente di configurare la strategia di verifica ed il comportamento di DigitalSign in fase di firma.

Il riquadro superiore permette di scegliere, per mezzo di una coppia di *radio button*, tra la modalità di verifica **STRONG** e la modalità **SOFT**.

- in modalità **STRONG** DigitalSign considera attendibili soltanto i certificati emessi da una CA inclusa nella '*trust list*'.
  La trust list è un elenco di certificati di CA costituito da:

- l’elenco ufficiale delle CA accreditate fornito da CNIPA
- l’elenco firmato di ulteriori CA attendibili (opzionale, si veda la prossima sezione)
- i certificati di CA eventualmente contenuti nella smartcard inserita

NOTA: in fase di verifica DigitalSign dichiara esplicitamente in quale di questi tre sottoinsiemi ha trovato il certificato di CA che ha emesso quello in corso di verifica.

- In modalità **SOFT** DigitalSign considera attendibili i certificati emessi da qualunque CA il cui certificato sia presente nel DB locale dei certificati. Questa modalità è comoda per test ed esperimenti, ma non dovrebbe essere usata in contesti di utilizzo effettivo.

Il riquadro sottostante presenta una serie di checkbox che controllano il comportamento in fase di verifica:

- **Verifica dello stato di sospensione/revoca dei certificati** – se attivo istruisce DigitalSign a verificare i certificati anche in merito all’eventuale stato di sospensione o revoca, tramite la relativa CRL (Lista di Sospensione o Revoca). Se questa opzione non è attiva DigitalSign mostra sempre un apposito messaggio di *warning* in occasione di ogni verifica.

- **Consenti aggiornamento automatico della CRL in fase di verifica** – se attivo consente a DigitalSign, in occasione della verifica di un certificato, di scaricare automaticamente la relativa CRL nel caso non disponga di una copia sufficientemente aggiornata.
  Se questa opzione non è attiva DigitalSign chiede conferma prima di operare lo scaricamento.
  La CRL viene in ogni caso prelevata dall’indirizzo codificato all’interno del certificato (CRL Distribution Point) e protetto dalla firma della CA.
  Naturalmente le CRL possono essere scaricate ed utilizzate solo se si dispone di un collegamento ad Internet.
  I protocolli utilizzati per lo scaricamento (impostati dai certificatori) sono HTTP, HTTPS o LDAP.

- **Forza rilettura di CRL anche non scadute, ogni <*x*> ore** – ogni CRL viene pubblicata dalla CA corredata di informazioni sul periodo di validità. Per le CA accreditate in Italia il periodo di validità varia da alcune ore sino a 24 ore, talvolta anche di più; la normale strategia di verifica è quella di considerare valida una CRL per tutto il tempo di validità dichiarata: se si verificano più certificati emessi dalla stessa CA, in generale solo la prima verifica provocherà l’effettivo scaricamento della CRL, dopo di che si continua ad utilizzare la copia scaricata localmente.
  Attivando questo checkbox, tuttavia, si istruisce DigitalSign ad anticipare il nuovo scaricamento della CRL trascorso un certo tempo dall’ultima volta in cui la lista era stata effettivamente scaricata, anche se essa è ancora nominalmente valida. Questo accorgimento consente di beneficiare con la massima tempestività di eventuali pubblicazioni anticipate da parte dei Certificatori.

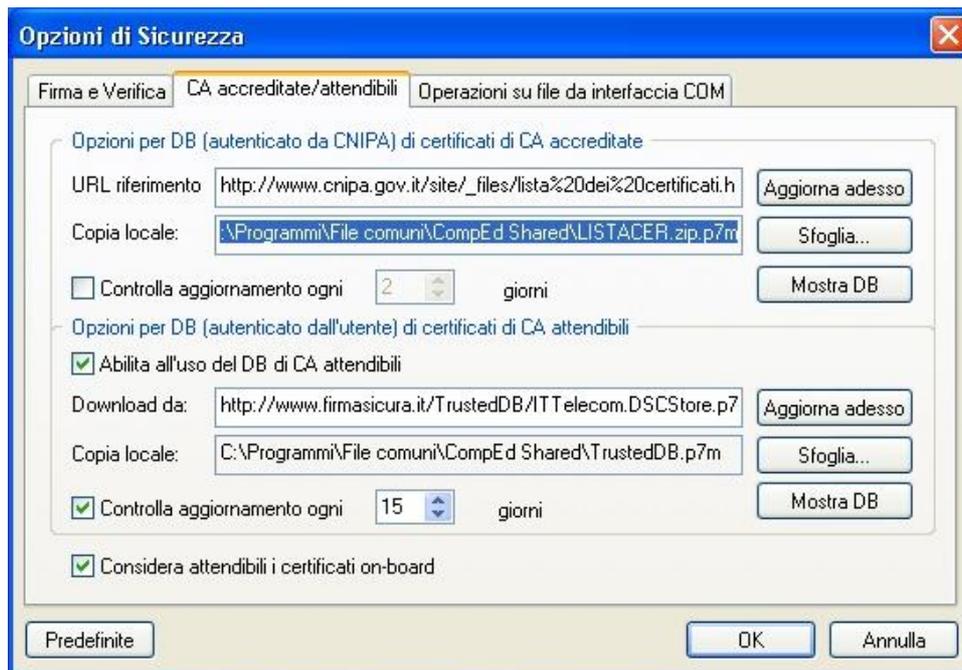
- **Verifica “nesting” del periodo di validità dei certificati** - questa opzione consente di attivare o disattivare una funzione di verifica soggetta a diverse interpretazioni da parte di diversi addetti ai lavori, che cerchiamo di spiegare.
  Si ricordi che un certificato intestato ad un soggetto è sempre emesso da un Certificatore, il quale lo firma utilizzando la propria chiave privata associata al proprio certificato di CA.
  Certa letteratura tecnica prescrive che in nessun caso un certificatore possa emettere un certificato il cui periodo di validità superi il periodo di validità del certificato di CA usato

per firmarlo (ciò appare ragionevole, perché quando il certificato di CA sarà scaduto il certificato in questione sarebbe ancora valido, ma la verifica non potrà comunque essere complessivamente superata a causa della non validità del certificato di CA). Questo concetto è chiamato *nesting* del periodo di validità (l'intervallo di validità del certificato emesso è totalmente compreso - *nested* - nell'intervallo di validità dell'emittente).
Tuttavia non si tratta di una regola imposta dagli standard, quanto di un vincolo implementato nei sistemi più autorevoli e diffusi: alcuni certificatori non osservano (o almeno non osservavano) questa regola mettendo in circolazione certificati la cui validità sconfina dai limiti di validità del certificato di CA.
Tornando alla configurazione di DigitalSign, se si attiva questa opzione i certificati che violano il principio del *nesting* non saranno considerati validi, altrimenti il problema verrà ignorato (fintanto che sarà ancora valido il certificato di CA relativo!).

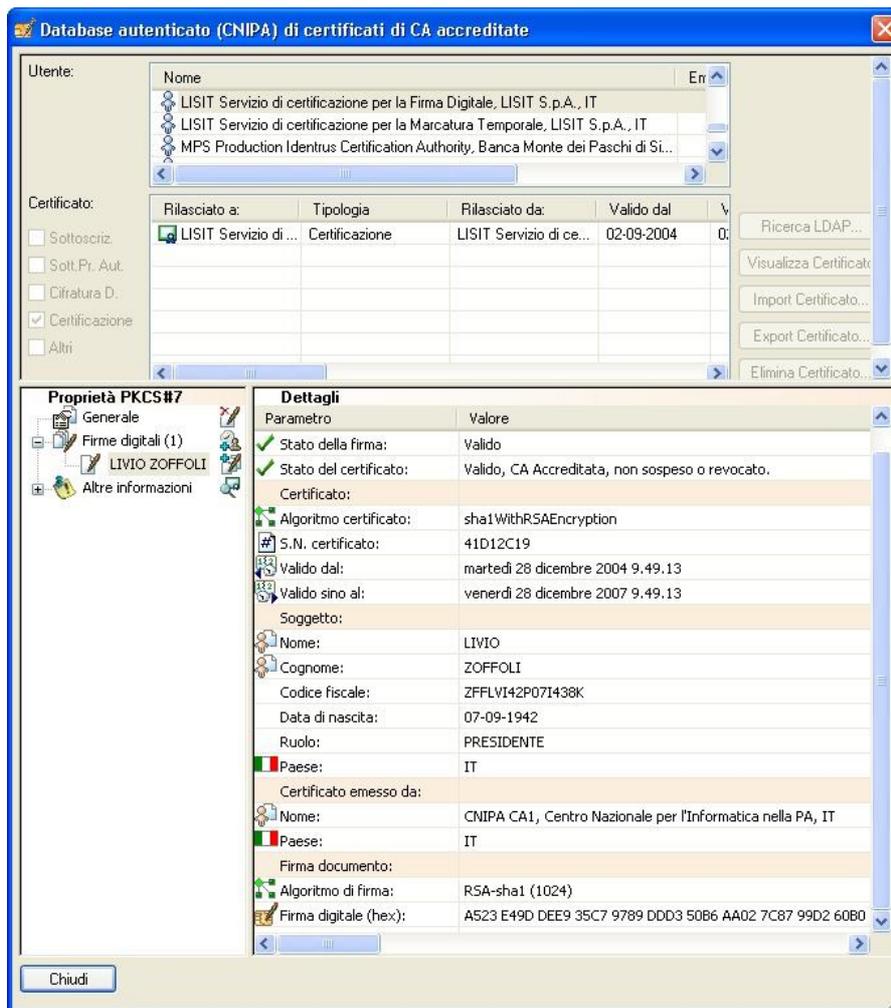
Seguono poi due parametri connessi con il periodo di validità legale delle Marche Temporali:

- **Validità Marche Temporali emesse prima del 3/12/2009 (ex DPCM 13/01/2004) <*x*> anni**
  Il DPCM 13/01/2004, all'art. 50, obbligava i certificatori a conservare copia di tutte le marche temporali emesse per un periodo minimo di 5 anni, oppure più a lungo a seguito di accordi con i clienti. Lo stesso decreto chiariva poi che i documenti firmati digitalmente e corredati di una marca temporale – ovviamente corrispondente ad un istante di tempo in cui la firma fosse realmente valida – mantenessero la proria validità anche dopo la scadenza del certificato usato per la sottoscrizione.
  Questo parametro consente di impostare il periodo di validità per le marche temporali in esame (per default 5 anni)
- **Validità Marche Temporali emesse dopo il 3/12/2009 (ex DPCM 30/03/2009) <*y*> anni**
  Il DPCM 30/03/2009, all'art. 49, modifica l'obbligo estendendolo a 20, ferma restando la facoltà di accordi certificatore-cliente per tempi di conservazione più lunghi.
  Questo parametro consente di impostare la durata di default pari a 20 anni o periodi ancora più lunghi.

La data del 3/12/2009 è quella di entrata in vigore dell'obbligo di conservazione per 20 anni stabilito dal DPCM 30/3/2009.
Quindi i parametri descritti servono a DigitalSign per decidere sulla durata effettiva della validità di una marca temporale rispetto all'emissione.
Se una marca temporale era stata emessa oltre 5 anni prima del 3/12/2009 allora il 3 Dicembre 2009 probabilmente la sua copia nell'archivio del certificatore non esiste più, dunque il documento non ha più il pieno valore probatorio.
Ma se la marca fosse stata emessa, per esempio, il 10 dicembre 2004 allora il 3 dicembre 2009 la copia d'archivio esisteva ancora e quindi l'obbligo di conservazione si estende ad un totale di 20 anni; e quindi, per i successivi 15 anni, il documento è ancora valido.

4.8.4.2 CA accreditate/attendibili

Questo pannello controlla i punti di riferimento utilizzati da DigitalSign per considerare attendibili i certificati sottoposti a verifica in modalità **STRONG**.

Il riquadro superiore – **Opzioni per DB (autenticato da CNIPA) di certificati di CA accreditate** – riguarda la fonte principale, sempre in uso in modalità **STRONG**: l'elenco di certificati di CA accreditate autenticato da CNIPA.
Il Centro Nazionale per l'Informatica nella Pubblica Amministrazione mantiene appunto un elenco dei certificati di tutte le CA accreditate per l'emissione di Certificati Qualificati e pubblica tale elenco ufficiale in forma elettronica, firmata digitalmente dal Presidente di CNIPA stesso.
Sia l'indirizzo Internet di pubblicazione che l'impronta del certificato del Presidente sono pubblicati nella Gazzetta Ufficiale.
Il campo contenente l'indirizzo per lo scaricamento di questo file è *read-only*, proprio perché l'indirizzo è univoco ed ufficiale. DigitalSign dispone poi di una copia locale di tale file, il cui percorso è modificabile con il bottone Sfoglia.
Ad ogni avvio DigitalSign apre la copia locale, verifica la firma del Presidente di CNIPA (eventualmente anche lo stato di revoca, se è attiva la relativa opzione), quindi estrae tutti i certificati contenuti e costruisce in memoria la '*trust list*' utilizzata per la verifica effettiva degli altri certificati.

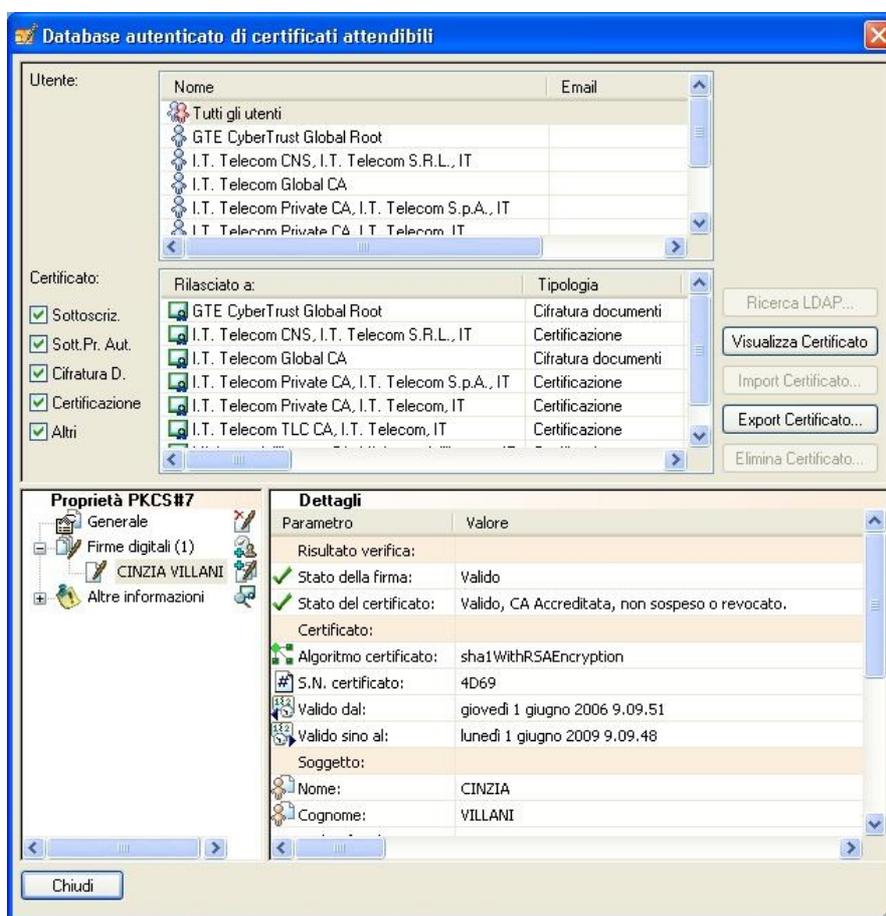
- Tramite il bottone **Aggiorna adesso** si provoca l'immediata rilettura dell'elenco CNIPA e la sovrascrittura della copia locale, nonché la verifica del nuovo file e la reinizializzazione della trust list con il nuovo contenuto.
- Il bottone **Mostra DB** apre una speciale finestra documento che mostra il contenuto del DB CNIPA tramite un viewer analogo a quello del DB locale, unitamente ai dati della sottoscrizione digitale del Presidente di CNIPA:

- Con il bottone **Chiudi** si torna alla finestra precedente.

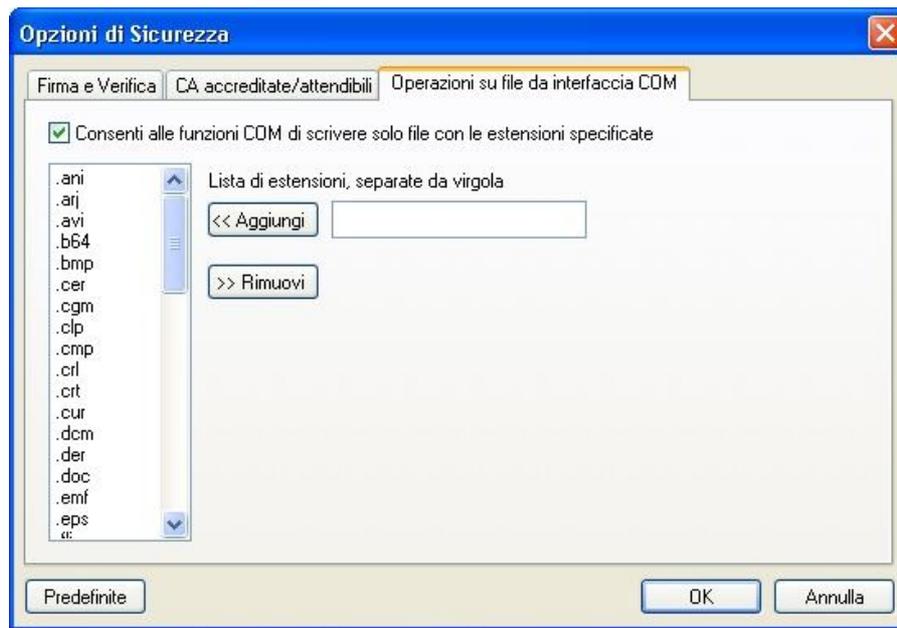
- È possibile configurare DigitalSign ad aggiornare periodicamente la propria copia locale, mediante il *checkbox* **Controlla aggiornamento ogni <*x*> giorni**. Si consiglia caldamente di attivare questa opzione, indicando un periodo relativamente breve (per esempio settimanale o quotidiano), soprattutto se si fa uso frequente del servizio di marcatura temporale.

Il riquadro sottostante – **Opzioni per DB (autenticato dall'utente) di certificati di CA attendibili** – consente di estendere l'insieme delle CA considerate attendibili, oltre a quelle accreditate da CNIPA.
Lo scopo di questo elenco aggiuntivo, che può essere messo in uso o meno per mezzo del checkbox Abilita all'uso del DB di CA attendibili, può essere:

- permettere all'utente, arbitrariamente, di considerare attendibili delle CA sperimentali o comunque estranee al circuito dell'accreditamento CNIPA
- consentire ad una organizzazione di considerare attendibili CA distinte da quelle accreditate (per esempio quelle che emettono certificati per l'Autenticazione, l'Attestazione o la Cifratura) usufruendo degli stessi livelli di sicurezza che DigitalSign adotta per le CA accreditate

L’utente – o il responsabile dell’organizzazione – predispone un elenco di certificati di CA da considerare attendibili e lo firma digitalmente con un Certificato Qualificato. Una volta pubblicato o distribuito tale file, configurato DigitalSign ad utilizzarlo, sarà possibile verificare positivamente i certificati emessi dalle CA incluse in questo elenco. Si noti però che DigitalSign riferirà con precisione che il certificato è considerato attendibile sulla base della firma del sottoscrittore dell’archivio autenticato.

I comandi di questo riquadro funzionano esattamente come quelli del riquadro superiore, salvo che anche l’indirizzo di download è modificabile.
Come si vede dall’esempio, questa tecnica è utilizzata anche dal Certificatore IT-Telecom per dichiarare attendibili – tramite la firma del Responsabile, Dott.sa Cinzia Villani – i certificati emessi da una serie di CA specializzate. Con **Mostra DB**:

Infine, in fondo alla finestra, il *checkbox* **Considera attendibili i certificati on-board**, se attivato, consente di verificare positivamente i certificati emessi da una CA il cui certificato si trova nella smartcard inserita.

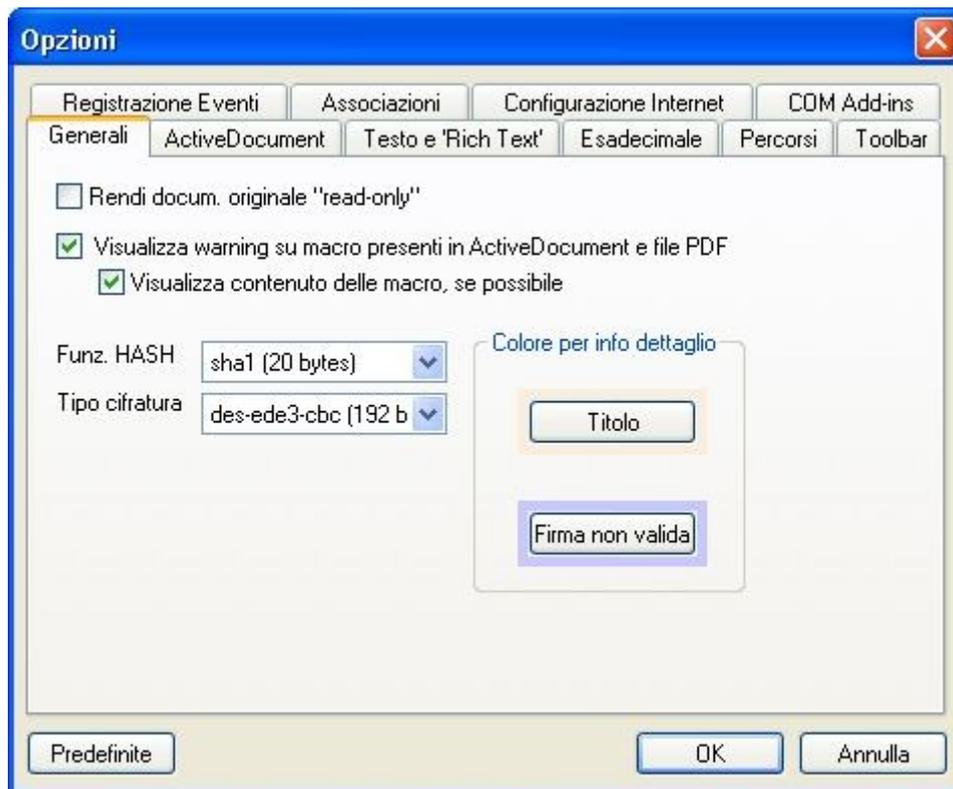
4.8.4.3 Operazioni su file da interfaccia COM

DigitalSign, come è noto, dispone di un'interfaccia (COM) tramite la quale altre applicazioni possono utilizzare i servizi di firma digitale, marcatura temporale, ecc. allo scopo di realizzare sistemi integrati.
Tuttavia le funzioni di questa interfaccia potrebbero essere utilizzate per introdurre nel sistema file eseguibili dannosi, come virus, trojans, e così via.
Questa finestra di dialogo consente di limitare la libertà di azione delle applicazioni client restringendo la loro possibilità di scrivere file.
Per attivare questa opzione di filtro occorre attivare il checkbox e cancellare/inserire le estensioni che si intende autorizzare.

4.8.5 Modulo di Gestione delle Opzioni

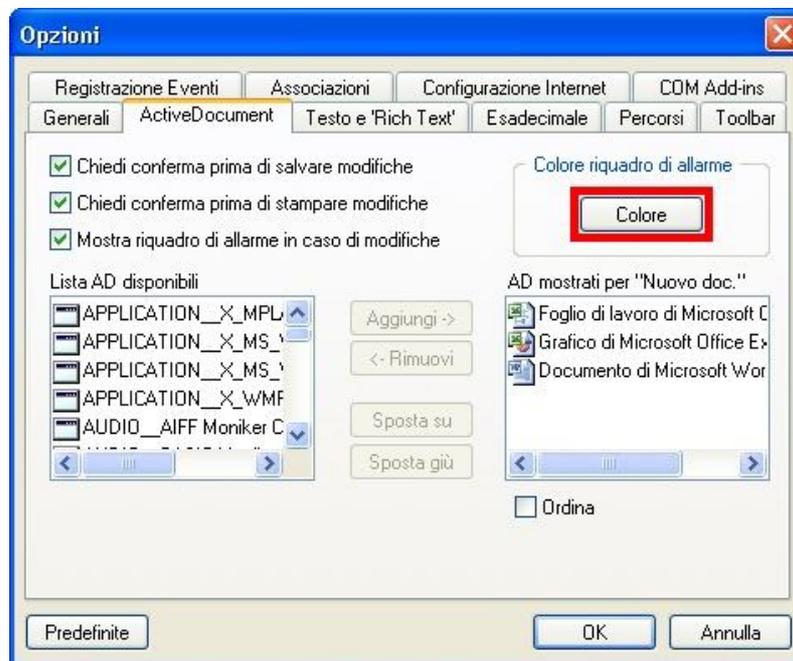
Questo modulo di configurazione presenta diverse cartelle per gestire altrettante serie di parametri.
Per tutte le cartelle sono disponibili i seguenti bottoni:

- **Predefinite** – ripristina i valori di default
- **OK** – salva le modifiche e chiude la finestra
- **Annulla** – chiude la finestra senza salvare le modifiche eventualmente apportate

4.8.5.1 Generali

Questa finestra di dialogo consente il controllo di alcuni parametri generali.

- **Rendi documento originale *read-only*** - se questo *checkbox* è attivato, i file corrispondenti ai documenti aperti da DigitalSign non verranno modificati da eventuali operazioni compiute nell'ambito della finestra documento associata (aggiunta o rimozione di firme digitali, di marche temporali, di destinatari di cifratura, ecc.). Occorrerà usare il comando del menu **File -> Salva documento con nome...**
- **Visualizza *warning* su macro presenti in doc. ActiveDocument e PDF -** se questo *checkbox* è attivo DigitalSign mostrerà, nel pannello dei dettagli della finestra documento, una riga di informazione sul rischio o sull'effettiva presenza di elementi variabili nel documento. Si veda anche la sezione dedicata al problema delle macro.
- **Visualizza contenuto delle macro, se possibile** - se questo *checkbox* è attivo (ed è attivo anche quello del punto precedente), nel caso il documento sia in un formato che DigitalSign è in grado di analizzare, il pannello dettagli della finestra documento mostrerà una lista esplicita delle macro rilevate. Si veda anche la sezione dedicata al problema delle macro.
- **Scelta funzione HASH** - per default mostra la funzione hash SHA-1, ma l'utente può selezionarne una diversa. Si ricordi cha attualmente la normativa italiana considera utilizzabili soltanto SHA-1 e RIPEMD-160 per le firme digitali a valore legale.
  NOTA: non tutti i dispositivi di firma sono in grado di generare firme digitali con le diverse funzioni hash disponibili.
- **Scelta del tipo da cifratura** - per default mostra la cifratura detta *triple-DES*, a 192 bit, ossia la più forte ed inviolabile tra quelle supportate; tuttavia è possibile scegliere altri algoritmi di crittografia del contenuto del documento. Si veda anche la sezione relativa alle modalità di cifratura.
- **Colore per informazioni dettaglio** - l'utente può controllare con questo bottone il colore in cui DigitalSign visualizza nell'area PKCS#7 della finestra documento i campi di informazione relativi a firme digitali la cui verifica non viene superata positivamente.

4.8.5.2 ActiveDocument

Questa finestra consente di controllare alcuni parametri relativi al comportamento di DigitalSign nella manipolazione di documenti aperti in una finestra documento tramite un viewer di tipo **ActiveDocument**.

Tre *checkbox* controllano il comportamento in presenza di modifiche apportate durante l'editing:

- **Chiedi conferma prima di salvare modifiche**
- **Chiedi conferma prima di stampare modifiche** – riguarda l'esecuzione di stampe di documenti modificati dopo l'apertura
- **Mostra riquadro di allarme in caso di modifiche** – se questo checkbox è attivo, in caso il documento venga modificato in fase di editing evidentemente le firme digitali preesistenti non saranno più valide; un riquadro lampeggiante di allarme informerà l'utente di questa circostanza.
  Un bottone **colore riquadro allarme** permette di configurare il "look" del riquadro di allarme di cui al punto precedente.

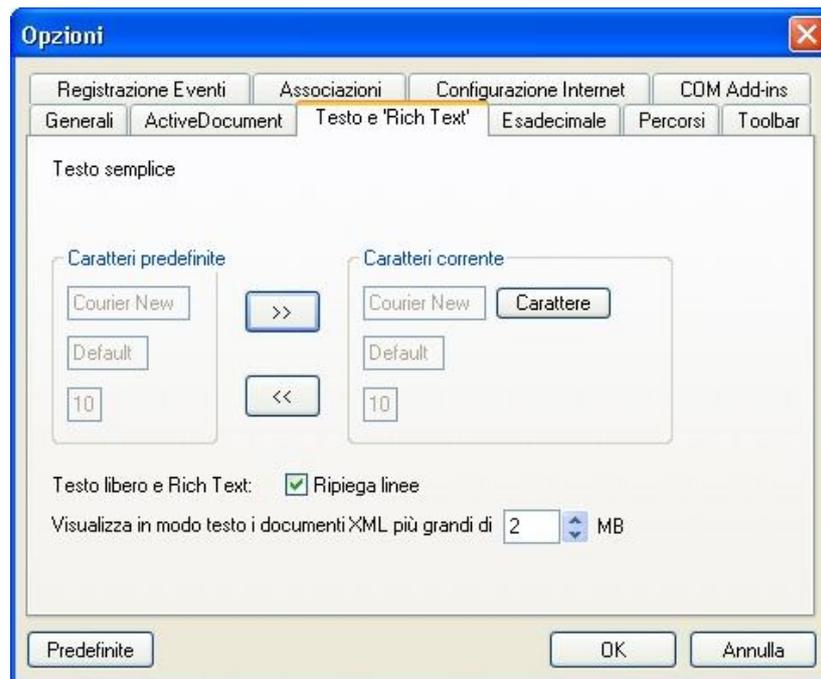
Nella parte bassa della finestra compaiono due riquadri tramite i quali è possibile configurare il sistema su quali applicazioni compatibili ActiveDocument, tra quelle installate nel sistema, sia possibile usare con DigitalSign.
Il riquadro di sinistra mostra tutte le applicazioni ActiveDocument ancora disponibili, quello di destra mostra quali applicazioni sono già state abilitate all'uso come viewer ActiveDocument per DigitalSign.

- Il bottone **Aggiungi** provoca il passaggio dell'applicazione correntemente selezionata nel riquadro di sinistra verso quello di destra (ossia inserimento tra le applicazioni abilitate)
- Il bottone **Rimuovi** provoca il passaggio dell'applicazione correntemente selezionata nel riquadro di sinistra verso quello di destra (ossia rimozione dalle applicazioni abilitate).
- Il bottone **Sposta su** provoca lo spostamento di una posizione verso l'alto dell'applicazione correntemente selezionata nel riquadro di destra.

- Il bottone **Sposta giù** provoca lo spostamento di una posizione verso il basso dell'applicazione correntemente selezionata nel riquadro di destra.

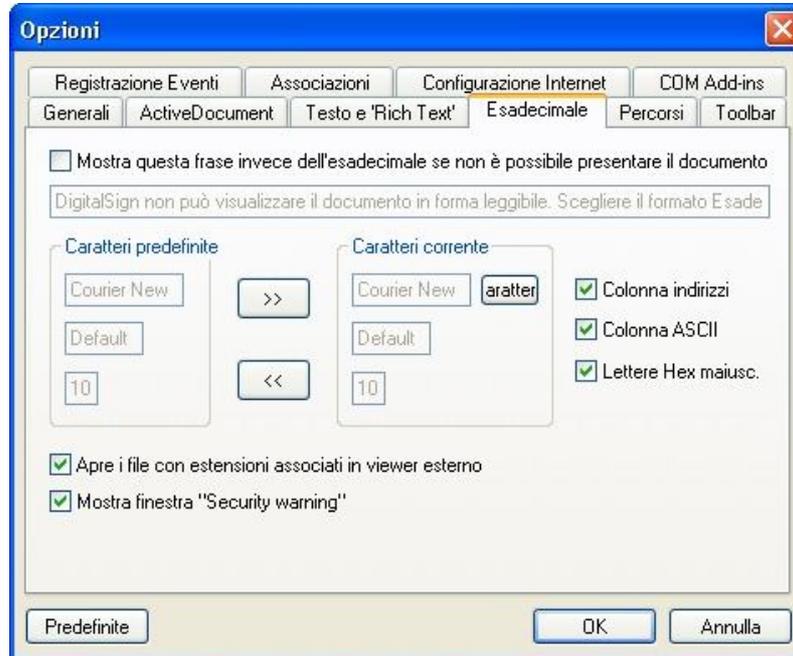
NOTA: la prima applicazione della lista del riquadro di destra è quella scelta per default quando si crea un nuovo documento.

4.8.5.3 Testo e "Rich Text"

Questa finestra di dialogo controlla alcuni parametri relativi al comportamento viewer per documenti di puro testo e per documenti *rich text*.

Due aree della finestra consentono di specificare un particolare font da utilizzare per la rappresentazione dei documenti di puro testo.
Il Font corrente è quello utilizzato per il documento correntemente aperto, il font di default è quello che verrà utilizzato per tutti i documenti di questo tipo.

- Tramite il bottone **[<<]** il font di default assume una configurazione identica a quella del font corrente.
- Tramite il bottone **[>>]** il font corrente viene riconfigurato in accordo con il font di default.
- Il *checkbox* **ripiega linee**, se attivo, istruisce DigitalSign a tagliare automaticamente le lunghe linee di testo che superano la larghezza della finestra e a riportarle su una linea successiva. Se il flag non è attivo l'utente dovrà agire sulla scroll-bar orizzontale per visualizzare tali linee lunghe.
- Il controllo **Visualizza in modo testo i documenti XML più grandi di <*x*> MB** serve a contrastare un limite di Internet Explorer (il viewer di default per i documenti XML) che provoca un abnorme consumo di memoria ed un conseguente progressivo decadimento delle prestazioni al crescere delle dimensioni dei documenti. Per ovviare a questo fenomeno DigitalSign limita l'uso di tale viewer ai file di dimensione contenuta, mostrando invece in formato di testo semplice quelli più grandi della soglia prefissata.

4.8.5.4 Esadecimale

Questa finestra di dialogo controlla alcuni parametri relativi al comportamento del viewer per dati binari di DigitalSign

Il *checkbox* **Mostra questa frase invece dell'esadecimale**, se attivo, fa sì che il viewer riporti semplicemente una frase informativa sull'impossibilità di manipolare il documento tramite un viewer specifico. Se il *checkbox* è disabilitato DigitalSign procede invece con la visualizzazione dei dati in formato esadecimale.
La frase specifica è impostabile dall'utente tramite l'*edit-box* sottostante.

Due riquadri sottostanti consentono di controllare il font da impiegare per la visualizzazione: Il font corrente è quello utilizzato per il documento correntemente aperto, il font di default è quello che verrà utilizzato per tutti i documenti di questo tipo.

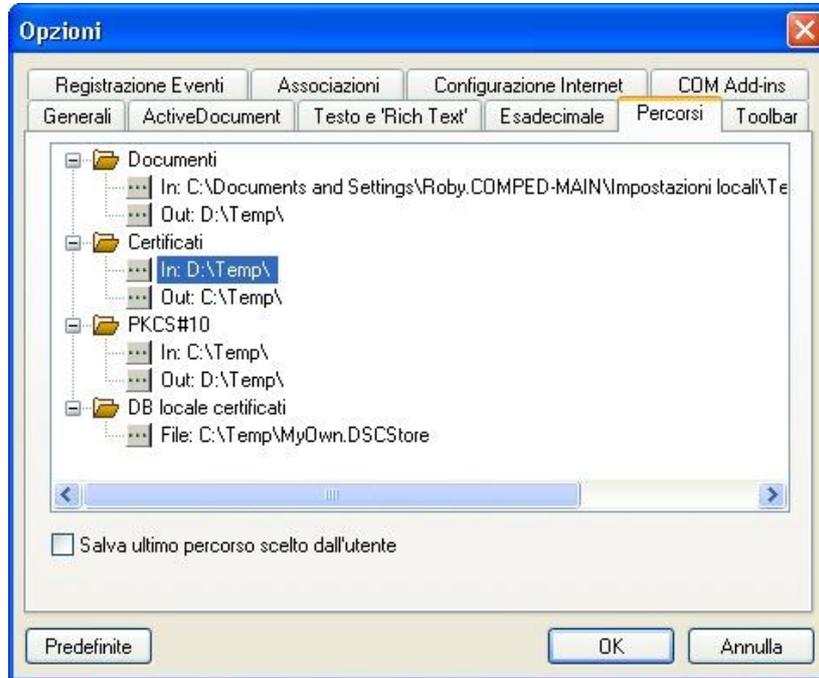
- Tramite il bottone **[<<]** il font di default assume una configurazione identica a quella del font corrente.
- Tramite il bottone **[>>]** il font corrente viene riconfigurato in accordo con il font di default.

Tre *checkbox* consentono di abilitare o disabilitare individualmente la visualizzazione, rispettivamente, della **colonna degli indirizzi** (offset), della **colonna ASCII**, l'utilizzo delle **lettere maiuscole** nella presentazione dei dati esadecimali.

Il checkbox **Apri i file con estensioni associate tramite viewer esterno**, se attivo, autorizza DigitalSign a utilizzare eventuali applicazioni registrate a livello di sistema per l'estensione del file in oggetto, come viewer esterno.

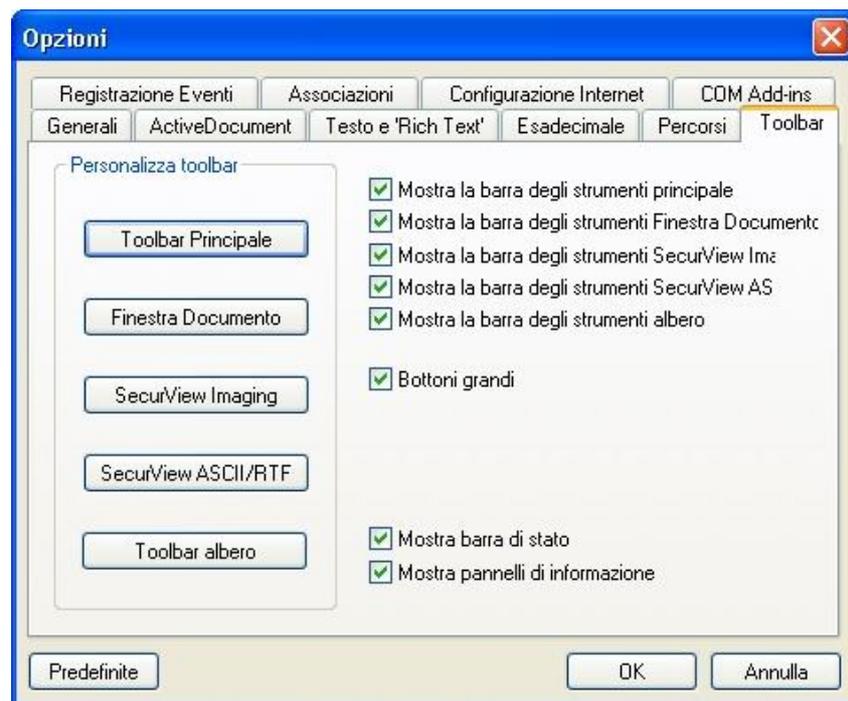
Il checkbox **Mostra security warning**, se attivo, istruisce DigitalSign a mostrare, prima dell'attivazione di un viewer esterno, una schermata di avvertimento sul ridotto livello di sicurezza offerto da un viewer di questo tipo.

4.8.5.5 Percorsi

Questa finestra di dialogo consente di controllare le posizioni di default in cui DigitalSign colloca i file di diverso tipo.

Alcuni parametri vengono aggiornati automaticamente, per esempio quando si salva un documento, ma modificando il parametro relativo di questa finestra l'utente può influire sulla proposta di default del sistema.

Il *checkbox* **Salva ultimo percorso scelto dall'utente**, se attivo, fa sì che il percorso effettivamente scelto dall'utente in una delle operazioni menzionate, venga salvato come percorso di default per le successive operazioni dello stesso tipo.

4.8.5.6 Toolbar

Questa finestra di dialogo consente di personalizzare le barre strumenti (toolbar) che DigitalSign presenta nelle diverse situazioni.

Sul lato destro della finestra sono elencati alcuni *checkbox* per controllare se DigitalSign debba o meno mostrare toolbar specifiche:

- **Mostra Toolbar principale** (quella mostrata inizialmente da DigitalSign anche quando nessuna finestra documento è aperta)
- **Mostra Finestra documento** (la toolbar specifica delle funzioni di DigitalSign mostrata all'interno di ogni finestra documento)
- **Mostra Securview Imaging** (quella associata al viewer per immagini raster)
- **Mostra Securview ASCII/RTF** (quella associata al viewer per documenti di puro testo e al viewer RTF)
- **Mostra Toolbar Albero** (quella verticale che appare sul separatore tra il pannello proprietà PKCS#7 e l'area dettagli della finestra documento)

Altri *checkbox* controllano il comportamento di DigitalSign relativamente alle toolbar:

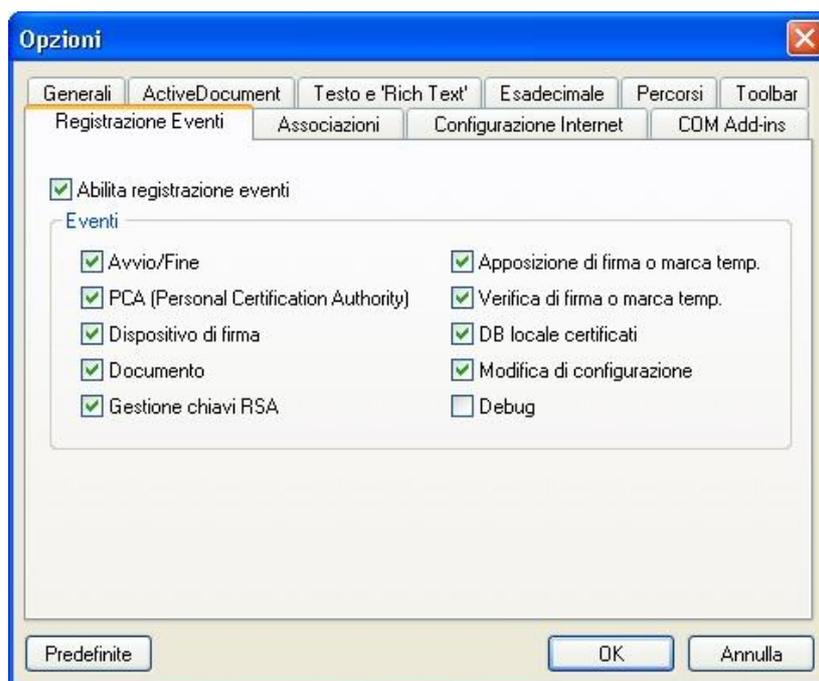
- **Bottoni grandi** - consente di controllare la dimensione dei bottoni delle toolbar
- **Mostra barra di stato** - controlla la visualizzazione della barra di stato in fondo alla finestra principale.
- **Mostra pannelli di informazione** - abilita o disabilita la visualizzazione dei pannelli informativi

Alcuni bottoni di comando permettono di personalizzare il contenuto delle diverse toolbar attraverso una specifica finestra di dialogo:

- **Toolbar principale** (quella mostrata inizialmente da DigitalSign anche quando nessuna finestra documento è aperta)
- **Finestra documento** (la toolbar specifica delle funzioni di DigitalSign mostrata all'interno di ogni finestra documento)
- **Securview Imaging** (quella associata al viewer per immagini raster)

- **Securview ASCII/RTF** (quella associata al viewer per documenti di puro testo e al viewer RTF)
- **Toolbar Albero** (quella verticale che appare sul separatore tra il pannello proprietà PKCS#7 e l'area dettagli della finestra documento)

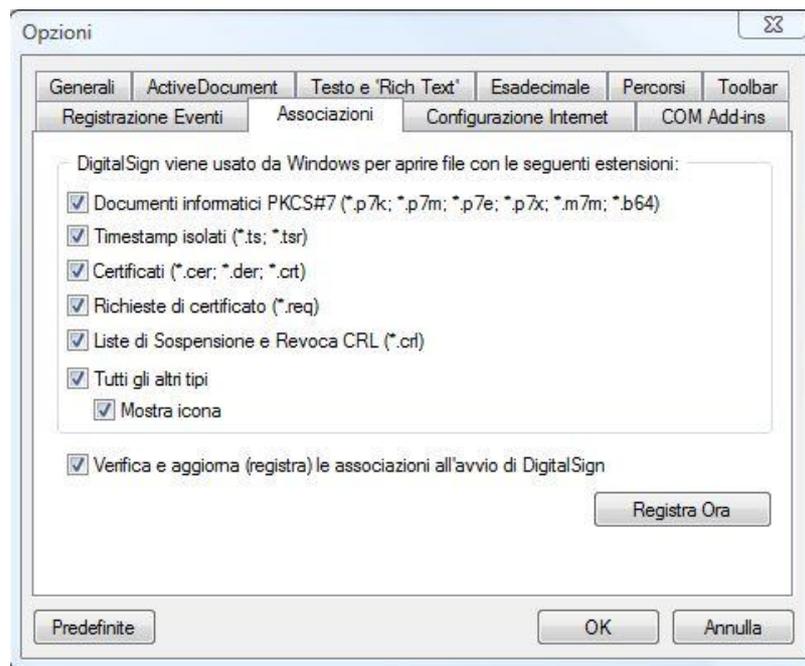
4.8.5.7 Registrazione Eventi

Questa finestra di dialogo permette all’utente di attivare/disattivare la registrazione degli eventi e, nel caso tale funzione sia attivata, di controllare quali categorie di eventi includere nella registrazione.

Il *checkbox* **Abilita registrazione eventi**, se attivo, fa sì che gli eventi significativi dell’attività di DigitalSign vengano effettivamente registrati.

Il riquadro sottostante, accessibile se il *checkbox* di abilitazione è attivo, consente di includere o escludere dalla registrazione le varie categorie di eventi disponibili.

NOTA: la categoria **Debug** merita particolare attenzione: se attivata provoca la scrittura di registrazioni molto dettagliate, soprattutto in materia di interfacciamento con le smartcard. L’effetto collaterale è che l’esecuzione rallenta significativamente, quindi va attivato solo in caso di necessità per analizzare situazioni problematiche.

4.8.5.8 Associazioni

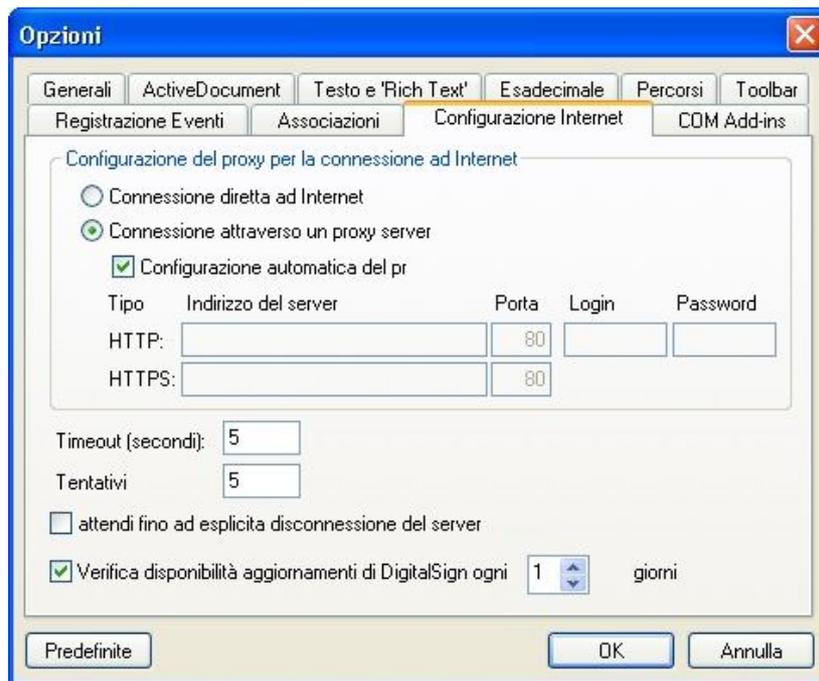
Questa finestra di dialogo consente di configurare le modalità secondo cui Windows fa uso di DigitalSign per gestire i file dei tipi compatibili con DigitalSign stesso.

Il primo riquadro permette di controllare le associazioni vere e proprie di DigitalSign ai file con le diverse estensioni specifiche. Questo significa che, agendo con doppio click (da Windows) su un file appartenente ad uno dei tipi selezionati, l'apertura avverrà per default con DigitalSign.

Esiste poi l'opzione **Tutti gli altri tipi**: quando questa è selezionata, se da una finestra di Windows Explorer si fa click con il tasto destro su un file di tipo generico, comparirà nel menu di apertura anche un **Apri con DigitalSign**.
Se poi è attiva anche l'opzione **Mostra icona**: il menu presenterà anche la tipica icona di DigitalSign.
Se l'operazione con il tasto destro viene effettuata a livello di una cartella invece che di un singolo file, si attiverà il meccanismo firma semiautomatica di file contenuti in una cartella dalla *shell* di Windows, si veda la relativa sezione.

Fuori dal riquadro si trova un altro checkbox, **Verifica e registra all'avvio di DigitalSign:** se questo è attivo DigitalSign riesegue ad ogni avvio la configurazione a livello di registro di sistema per tutte le associazioni qui configurate (utile nel caso in cui altre applicazioni nel frattempo avessero modificato la configurazione)

Esiste un bottone di comando specifico, **Registra ora**, che provoca la registrazione immediata in Windows della configurazione appena completata.

4.8.5.9 Configurazione Internet

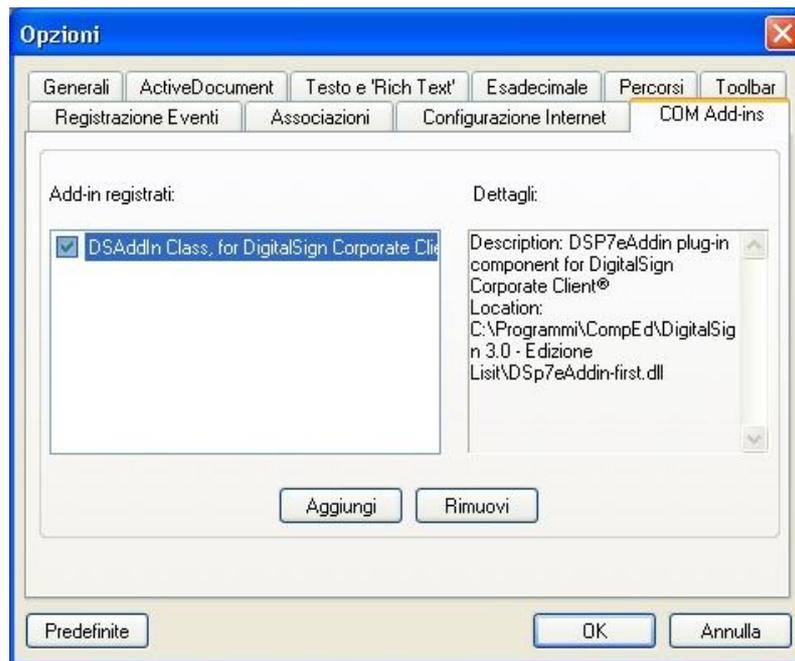
Questa finestra di dialogo consente di configurare la modalità in cui DigitalSign deve accedere ad Internet, per le operazioni che lo richiedono (marcatura temporale, scaricamento degli elenchi autenticati di certificati accreditati/attendibili, consultazione delle CRL, ...).

I *radio button* del primo riquadro consentono di scegliere tra una connessione diretta (nel caso di configurazioni di rete relativamente libere) o attraverso un *proxy* aziendale.
Nel secondo caso la scelta di operare una configurazione automatica (che eredita la configurazione di Internet Explorer) risolve la gran parte delle situazioni.

NOTA: l'eventuale configurazione del proxy ha effetto solo sulle connessioni via http e https, non sulle connessioni in LDAP.

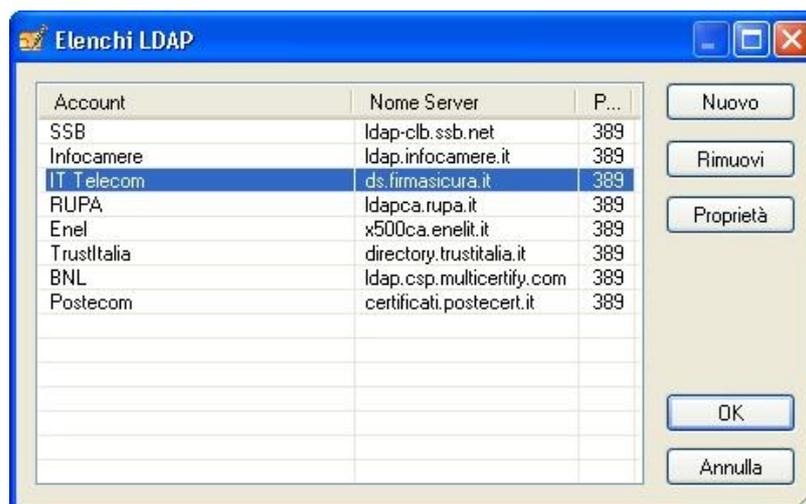
Ove fosse necessario configurare parametri specifici, incluse le credenziali di accesso, può essere utile rivolgersi all'amministratore di sistema.
Per testare il risultato della configurazione il modo più semplice è utilizzare la funziona Aggiorna Adesso della finestra delle **Opzioni di Security -> CA Accreditate/attendibili**, riquadro del DB CNIPA: si tratta di un file sempre disponibile, accessibile attraverso il protocollo **http**.

L'ultimo *checkbox* Verifica disponibilità aggiornamenti di DigitalSign ogni <x> giorni consente di mantenere aggiornata la propria installazione, tramite un accesso al server di CompEd.

4.8.5.10 COM Add-Ins

Questo pannello serve alla gestione di moduli Add-In per DigitalSign.
In generale la presenta può presentarsi vuota oppure contenere la lista degli Add-in correntemente installati:

- Con il bottone **Aggiungi** è possibile installare un nuovo Add-in (si faccia riferimento alla documentazione specifica dell’add-in che si intende installare)
- Con il bottone **Rimuovi** si opera la disinstallazione dell’add-in selezionato dalla lista

4.8.6 Modulo di Configurazione dei servizi di accesso agli elenchi di certificati LDAP

Questa finestra di dialogo consente di configurare i servizi di consultazione degli elenchi di certificati in linea.

È possibile inserire diversi servizi, che corrispondono ad altrettanti server LDAP, in generale uno per ogni certificatore ritenuto di interesse.
In seguito all’installazione DigitalSign già contiene i servizi di principale interesse (tuttavia i certificatori possono modificare i parametri, per cui sarà cura dell’utente rivedere la configurazione).

Si ricorda che ogni certificatore accreditato è tenuto per legge, tra l'altro, a:

- predisporre un Manuale Operativo approvato da CNIPA e a pubblicarlo in Internet
- dichiarare nel Manuale Operativo l'indirizzo Internet del proprio server LDAP
- comunicare a CNIPA l'indirizzo di pubblicazione del proprio Manuale Operativo, per cui su www.cnipa.it sono reperibili tutte le informazioni necessarie e in caso di incompletezza sarà possibile contattare i riferimenti.

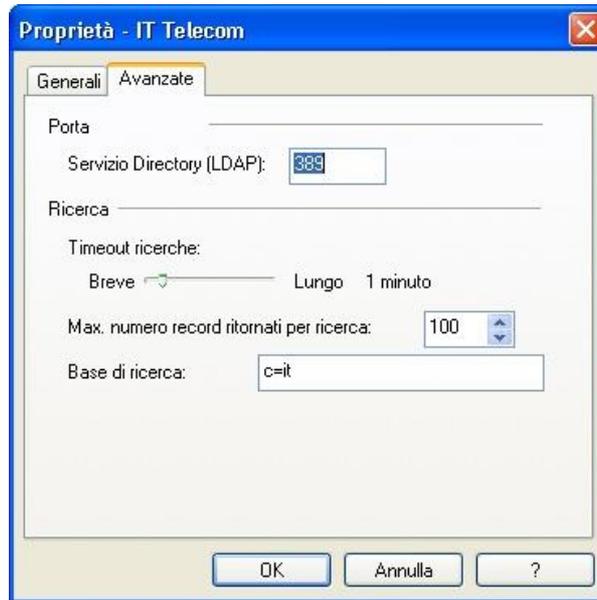
  - Il bottone **Nuovo** crea una nuova entry e conduce alla finestra di dialogo per la compilazione dei relativi parametri.
  - Il bottone **Rimuovi** elimina il servizio selezionato
  - Il bottone **Proprietà** conduce alla finestra di dialogo per la revisione dei parametri relativi al servizio selezionato

  - Il bottone **OK** salva le modifiche apportate e chiude la finestra
  - Il bottone **Annulla** chiude la finestra senza salvare le eventuali modifiche.

4.8.6.1 Finestra di configurazione di un servizio LDAP

Questa finestra di dialogo è in effetti organizzata in due distinte cartelle, la prima delle quali è **Generali**:

- Il **Nome Simbolico (Account)** viene attribuito dall'utente ed ha solo un significato locale, per distinguere i vari servizi attivi in DigitalSign. Tipicamente si usa il nome del certificatore che gestisce il server.
- Il **Nome del server** è in pratica l'indirizzo Internet a cui il server risponde. Questa informazione è pubblicata dal certificatore che gestisce ogni servizio
- Il *checkbox* **Questo server richiede logon** va attivato se il server in oggetto richiede che l'utente sia preventivamente registrato ed in tal caso occorre fornire anche il **nominativo** e la **password** necessari per l'accesso

La cartella **Avanzate** si presenta come segue:

- Il **Servizio Directory** è in effetti il numero di porta, un parametro specifico del server. Il valore 389 è usato di norma da tutti i server LDAP, ma in casi particolari può essere necessario un valore diverso (consultare il gestore)
- Il **Timeout ricerche** indica il tempo massimo durante il quale DigitalSign attenderà una risposta prima di considerare la ricerca fallita. Si agisce spostando il cursore a destra o sinistra per allungare o abbreviare l'intervallo
- Il **Massimo numero record ritornati per ricerca** limita il flusso di informazioni trasferite nel caso si introduca una chiave di ricerca troppo ampia, soddisfatta da molti record. Da notare che molti server limitano comunque il numero di record ritornati
- La **Base di Ricerca** è una stringa usata per limitare la ricerca a record di una specifica categoria. I server gestiti dai certificatori accreditati CNIPA di norma esigono che la base di ricerca sia "**c=it**", altrimenti non ritornano alcun risultato.

4.8.7 Modulo di Configurazione dei servizi di Marcatura Temporale

Questo modulo permette di visualizzare, aggiungere od eliminare gli account di marcatura temporale utilizzabili.
DigitalSign consente di interagire con diversi *provider* di servizi di marcatura temporale, l'utente deve creare e configurare un *account* per ogni fornitore che intende utilizzare.
La schermata mostrata in figura visualizza tutti gli account correntemente configurati:

- Con il bottone **Nuovo** si passa all'inserimento di un nuovo account, per mezzo di una ulteriore finestra di dialogo
- Con il bottone **Rimuovi** è possibile eliminare l'account selezionato
- Il bottone **Proprietà** mostra le caratteristiche dell'account selezionato, con la possibilità di modificarle per mezzo di una ulteriore finestra di dialogo
- Il bottone **Predefinito** permette di indicare l'account selezionato come quello predefinito da utilizzare con tutti i comandi di marcatura temporale. Il bottone non è accessibile se l'account selezionato è già il predefinito (oppure l'unico disponibile). L'account attualmente predefinito viene indicato nella lista.
- Il bottone **TSA report** consente – per i servizi che supportano tale funzione, attualmente soltanto Infocamere – di ottenere un rapporto sul credito di marche temprale residuo

- Il bottone **OK** chiude la finestra registrando le modifiche eventualmente apportare.
- Il bottone **Annulla** chiude la finestra senza salvare le modifiche.

4.8.7.1 Finestra di configurazione per un account di Marcatura Temporale

Quando si richiede la creazione di un nuovo account di Marcatura Temporale occorre innanzitutto assegnare un nome all’account e scegliere il “protocollo”. In particolare tale protocollo consiste nella modalità di accesso: i diversi certificatori operativi in Italia erogano il proprio servizio attraverso apposite servlet proprietarie, che richiedono quindi differenti configurazioni.

Attualmente sono supportati i seguenti protocolli:

- Specifiche RFC3161 (collegamento diretto, privo di servlet intermediaria)
- Specifiche Infocamere TSA
- Specifiche IT-Telecom
- Specifiche Actalis TSA

La schermata di configurazione per la modalità **RFC3161** si presenta come segue:

L'utente deve fornire tutti i dati, soprattutto l'indirizzo del server ed il numero di porta.

La schermata di configurazione per la modalità **Infocamere** si presenta come segue:

L'indirizzo della *servlet* è già preconfigurato, tuttavia l'utente dovrebbe sempre verificarne la correttezza, poiché il provider tende a modificarlo di quando in quando.
Il **Nome di logon** e la **Password** devono naturalmente essere forniti dall'utente.

La schermata di configurazione per la modalità **IT-Telecom** si presenta come segue:

Come si vede è del tutto analoga a quella Infocamere, ma è possibile introdurre anche un valore per la policy.
Poiché IT-Telecom fornisce il servizio attraverso diversi server per differenti categorie di utenti è necessario prestare attenzione e configurare il servizio sulla base delle informazioni fornite dal provider.

La schermata di configurazione per la modalità **Actalis** si presenta come segue:

Del tutto analoga alle precedenti.

4.8.8 Modulo per la generazione di una CRL

Questo modulo funzionale, appartenente alla Personal Certification Authority, consente di produrre una lista di revoca da utilizzare per la verifica di certificati prodotti appunto tramite la PCA.

La finestra di gestione, accessibile solo se è inserita – ed in stato di logon – una smartcard contenente un certificato di CA, si presenta come in figura:

La tabella mostra tutti i certificati attualmente contenuti nel DB locale generati con il certificato di CA contenuto nel dispositivo di firma correntemente inserito.

La tabella contiene le seguenti colonne:

- numero di serie del certificato
- nominativo del titolare del certificato
- inizio validità nominale
- termine validità nominale
- data dell'eventuale sospensione/revoca
- indicatore dello stato del certificato (R=Revocato, V=Valido)

La prima volta che si accede a questo modulo la tabella mostrerà tutti i certificati in stato di validità; quando si accederà a questa funzione in seguito, dopo aver generato una lista contenente almeno un certificato in stato di revoca, la tabella continuerà a mostrare lo stato imposto in precedenza (naturalmente le informazioni vengono prelevate dall'ultima CRL caricata nel DB locale), per cui si potranno aggiornare i dati e quindi creare una nuova copia aggiornata della CRL
Si veda l'esempio corrispondente a due certificati revocati:

Alcuni bottoni comando situati sotto la tabella consentono di operare sulla tabella stessa:

- **Mostra Certificato di CA -** visualizza il certificato corrispondente alla chiave di certificazione contenuta nel dispositivo di firma per il quale si sta costruendo la CRL
- **Mostra selezionato** - mostra il certificato correntemente selezionato nella tabella
- **Revoca -** cambia lo stato del certificato selezionato
- **Annulla revoca** - ripristina lo stato di *attivo* per il certificato selezionato

Un altro riquadro consente di configurare alcune opzioni per la produzione del file che rappresenta la CRL:

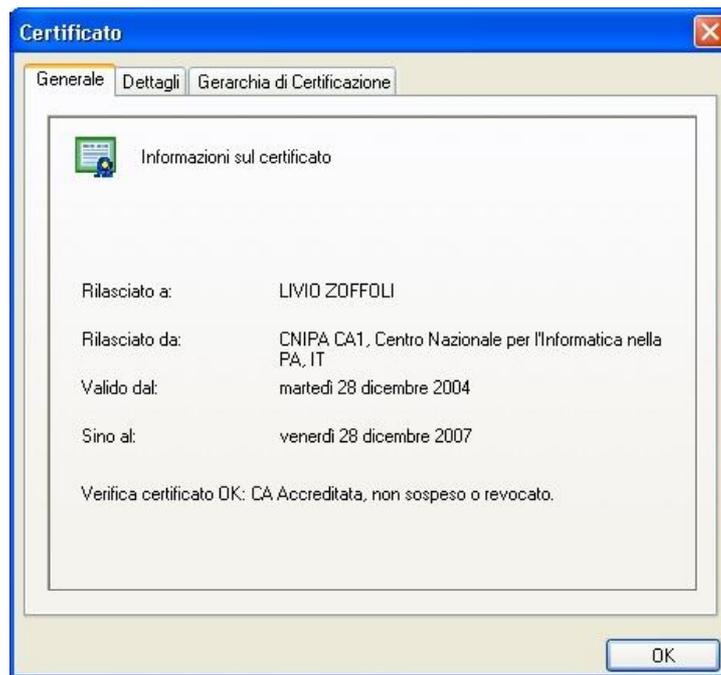
- **Periodo di validità CRL <x> giorni**: tale termine viene registrato all'interno della CRL, così che in fase di consultazione sia possibile verificare se la lista è ancora attuale oppure se è obsoleta
- **Salva CRL**: l'utente deve dichiarare un nome per il file completo di percorso, eventualmente utilizzando il bottone **Sfoglia**
- **Formato Base64**: attivando questo checkbox la lista verrà esportata in tale formato

Il bottone **Genera** provoca la creazione della CRL, che conterrà i riferimenti a tutti i certificati che nella tabella riportano lo stato di revocato o sospeso. La lista verrà anche caricata nel database locale dei certificati, dal quale potrà poi essere gestita mediante l'apposito modulo di gestione.

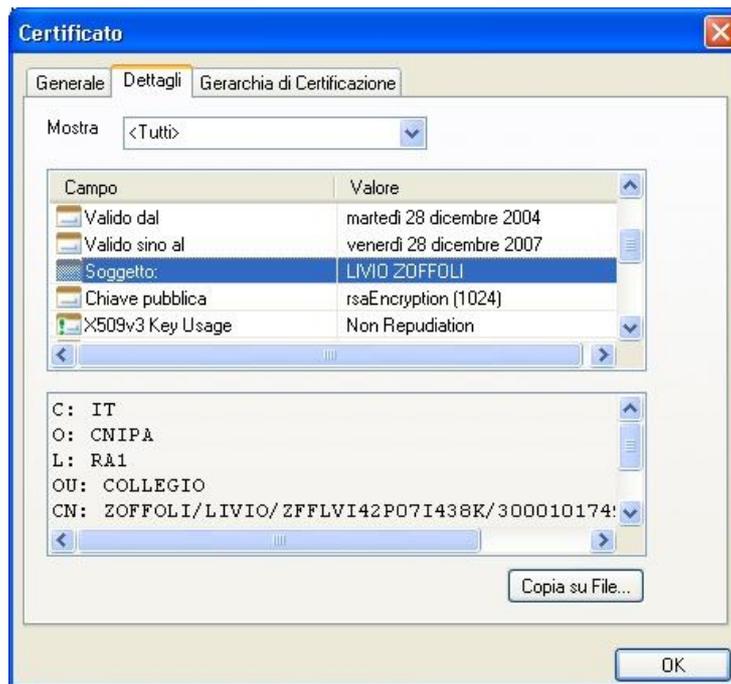
Si noti che per mettere in esercizio la CRL prodotta è necessario che essa venga poi resa accessibile alla URL scritta in tutti i certificati prodotti dalla CA in questione, cioè quello che si trova esplicitato nel file .INI, si vedano i dettagli a proposito della Personal Certification Authority. Naturalmente è necessario ripetere questa operazione prima di ogni scadenza della validità della CRL, evitando che gli utenti trovino alla URL predefinita una CRL scaduta.

4.8.9 Modulo di visualizzazione di un Certificato

Questo viewer viene utilizzato per presentare il contenuto di un certificato o di una richiesta di certificato.
Nel caso del certificato, in generale, la visualizzazione è organizzata in tre distinte cartelle:

Generale

Le informazioni mostrate in questa finestra sono:

- **Rilasciato a -** il titolare del certificato e quindi della relativa coppia di chiavi
- **Rilasciato da -** il fornitore di servizi di certificazione che lo ha rilasciato (eventualmente un organo interno all'organizzazione, qualora si operi mediante la Personal Certification Authority)
- **Valido dal -** l'inizio del periodo di validità, imposto dall'autorità di certificazione
- **Sino al -** termine del periodo di validità, imposto dall'autorità di certificazione
- **Verifica certificato -** lo stato di validità del certificato, in termini di verifica della relativa firma. IL caso più normale, come quello in figura, riporta la verifica superata positivamente, il fatto che il certificato in esame è stato emesso da una CA accreditata (presso CNIPA), il fatto che non è sottoposto a revoca o sospensione.
  Diciture specifiche informano invece l'utente se la verifica dello stato di revoca non è attivo o se il certificato è considerato valido ma è stato emesso da una CA diversa da quelle accreditate.

Dettagli

La finestra presenta in alto un campo con etichetta **Mostra** che permette di scegliere se la visualizzazione deve riguardare tutte le informazioni (per default) oppure le sole "proprietà".
Il riquadro sottostante contiene una tabella di entry, ciascuna delle quali rappresenta un campo del certificato ed il relativo valore. Poiché alcuni valori (per esempio la chiave pubblica) sono troppo grandi per essere contenuti nella colonna destra della tabella, la finestra contiene un ulteriore riquadro nel quale vengono riportate per esteso le informazioni contenute nel campo del certificato correntemente selezionato.

I campi principali sono:

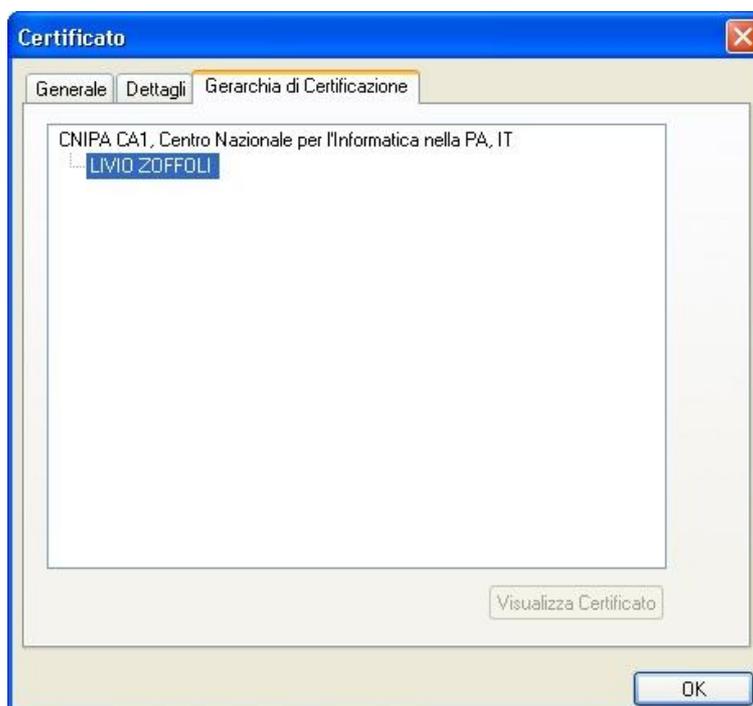
- **Versione -** numero di versione del file che contiene il certificato
- **Num. di serie -** un numero di serie univoco assegnato al certificato da parte della Certification Authority che lo ha generato. È espresso in notazione esadecimale.
- **Algoritmo di firma -** la specifica dell'algoritmo standard impiegato per la firma digitale che sigilla il certificato
- **Emesso da –** La Certification Authority le informazioni sul soggetto che ha emesso il certificato
- **Valido dal -** la specifica dell'inizio del periodo di validità del certificato
- **Valido sino al -** la specifica del termine del periodo di validità del certificato
- **Soggetto** - le informazioni sul soggetto titolare del certificato
- **Chiave pubblica** - il contenuto effettivo della chiave pubblica oggetto del certificato, espressa in notazione esadecimale
- **Algoritmo di impronta** - la specifica della funzione hash impiegata per calcolare l'impronta su cui è stata poi calcolata la firma digitale del certificato
- **Impronta** - il contenuto effettivo dell'impronta del certificato, espresso in notazione esadecimale.

In generale in certificato contiene poi altri elementi di informazioni, soprattutto se si tratta di un certificato generato in accordo con la normativa Italiana sulla firma digitale (si veda la Deliberazione CNIPA 4/2005).

Tra tali elementi di informazione si segnalano in particolare:

- **X509v3 Key Usage** – ossia la specifica sulla tipologia della chiave riferita dal certificato stesso. I certificati per la firma digitale “forte” in Italia devono avere unicamente il valore “Non repudiation” in questo campo.
- **X509v3 CRL Distribution Points** – è l’indirizzo Internet a cui si trova la lista dei certificati sospesi e revocati pubblicata dalla CA che ha emesso questo certificato.

Il bottone **Copia su file** permette di esportare il certificato su un file (.CER) in formato X.509 (DER encoded) scelto dall'utente.

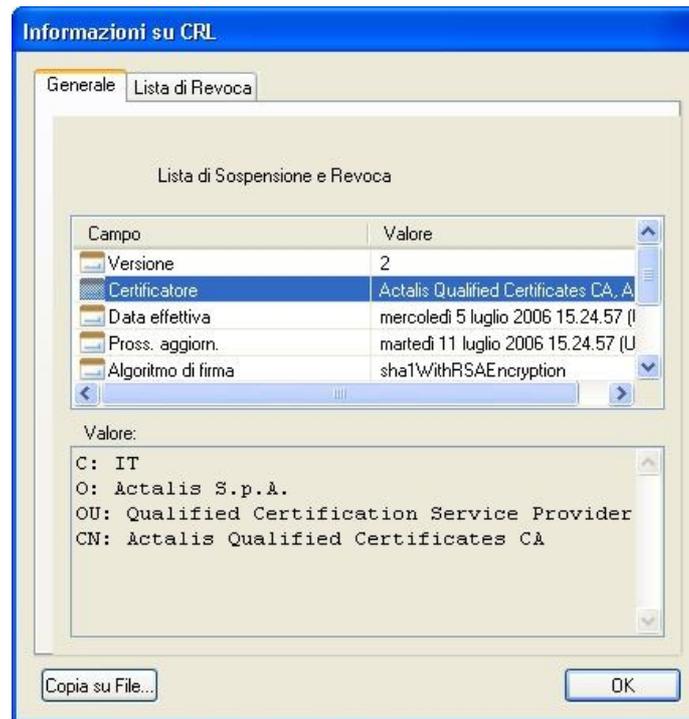
Gerarchia di Certificazione

Questa schermata mostra visivamente la catena di certificazione di un certificato di chiave pubblica.

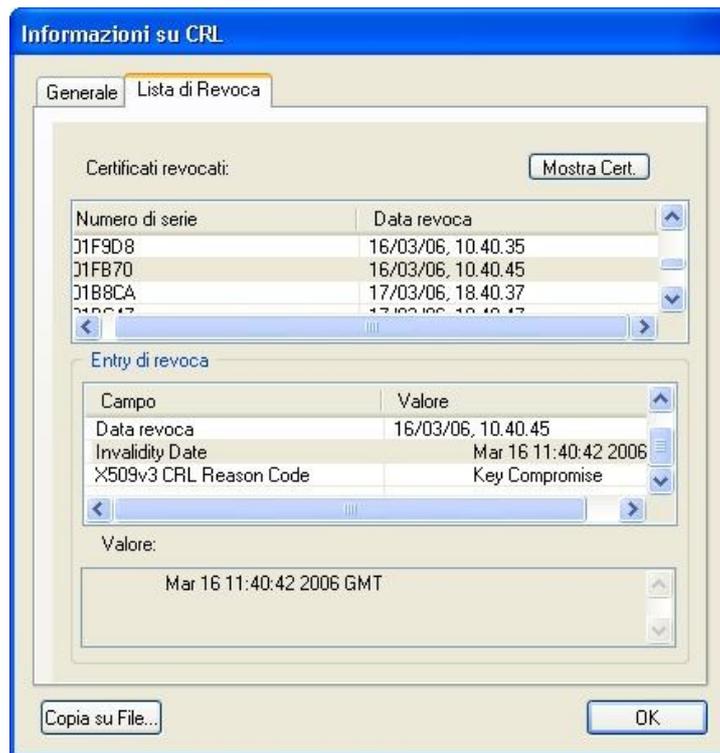
Ogni certificato deve infatti essere firmato digitalmente dalla Certification Authority che lo emette, il cui certificato deve a sua volta essere disponibile per la verifica e potrebbe a sua volta essere stato emesso da un altro soggetto di livello più elevato.
Si risale così una catena sino al raggiungimento di un certificato di livello root, firmato da se stesso.

Lo schema dell’infrastruttura italiana prevede solo due livelli, come in figura.

Selezionando il certificato del livello superiore diventa disponibile il bottone **Visualizza Certificato**, che consente di esaminare il certificato della CA emittente.

4.8.10 Modulo di visualizzazione di una Lista di Sospensione o Revoca

Questa finestra è organizzata in due cartelle, la prima della quale mostra le informazioni generali relative alla lista di revoca:

La tabella del primo riquadro mostra tutti gli elementi fondamentali della CRL, in particolare il nominativo della Certification Authority che l'ha emessa, la data effettiva di emissione, la data pianificata da Certificatore per l'emissione del prossimo aggiornamento.
Il riquadro inferiore mostra gli eventuali dettagli disponibili per l'elemento del primo riquadro correntemente selezionato

La seconda cartella mostra invece il contenuto effettivo della lista:

Si noti che una CRL contiene unicamente i numeri di serie come riferimenti ai certificati veri e propri, non contiene i certificati completi. Quindi è possibile sapere, dato un certificato, se esso è incluso nella lista (ricercandone il numero di serie), ma non è possibile conoscere le identità dei titolari di tutti i certificati revocati semplicemente disponendo della lista.

Tuttavia, se nel DB locale è presente un certificato corrispondente alla entry correntemente selezionata, il bottone **Mostra Certificato** lo apre per la visualizzazione.

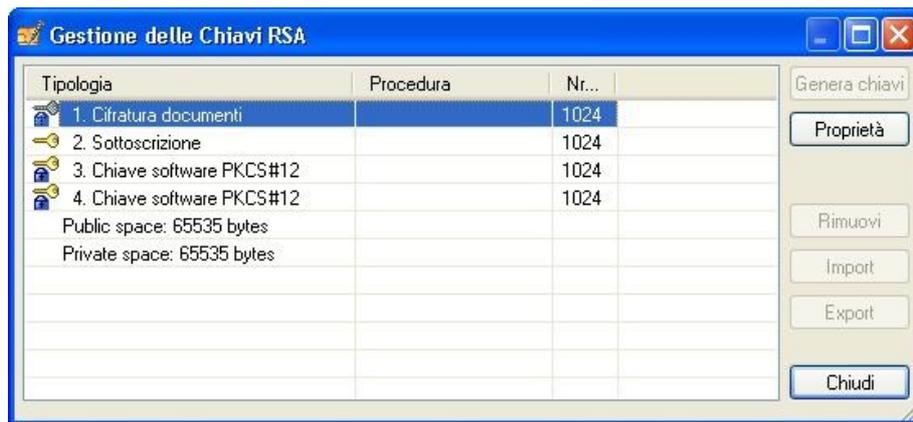
Il riquadro superiore contiene la lista effettiva: una tabella le cui colonne rappresentano, rispettivamente, i numeri di serie dei certificati e la data di sospensione o revoca.

Il riquadro **Entry di revoca** mostra tutti i dettagli relativi alla riga della tabella superiore correntemente selezionata; numero di serie del certificato, data e ora della sospensione o revoca, il codice e descrizione dell'operazione impostato dal certificatore per quel certificato.

Il riquadro **Valore** mostra una ulteriore espansione del dettaglio correntemente selezionato nel riquadro delle entry di revoca.

Da entrambe le cartelle, con il bottone **Copia su File** è possibile esportare la CRL su un file esterno, con **OK** si chiude la finestra.

4.8.11 Modulo di gestione delle coppie di chiavi RSA

Questo modulo consente di operare sull’insieme di coppie di chiavi presenti in un dispositivo di firma:

La tabella mostra una riga per ogni coppia di chiavi disponibile nel dispositivo, ma – come in questa figura – possono comparire anche una o più chiavi aggiuntive definite come Chiave software PKCS#12: si tratta in tal caso di coppie di chiavi che non si trovano fisicamente nel dispositivo ma sono invece importate da file PKCS#12 (operando dal menu **Dispositivo di firma -> Configurazione** ed utilizzando la cartella **Caricamento file PKCS#12**).

Per ognuna delle coppie di chiavi vengono visualizzate le seguenti informazioni:

- l'icona che rappresenta la tipologia
- la tipologia in esteso (a meno che non si tratti di chiavi software, come spiegato sopra)
- l'eventuale identificatore della procedura automatica (solo per le coppie di chiavi di sottoscrizione mediante procedura automatica): questa colonna è mantenuta per compatibilità con dispositivi di firma personalizzati con vecchie edizioni di DigitalSign
- la lunghezza delle chiavi, espressa in bit

Sono disponibili alcuni bottoni comando:

- **Genera chiavi -** conduce ad una finestra di dialogo che assiste alla creazione di una nuova coppia di chiavi. Questo comando è abilitato solo se si opera con un dispositivo che effettivamente consente la generazione.
- **Proprietà –** conduce ad una ulteriore finestra di dialogo che illustra proprietà di dettaglio della coppia di chiavi selezionata.
- **Import -** consente di importare da un file in formato PKCS#12 una coppia di chiavi di cifratura. In pratica è una operazione di *restore*, mentre l'export è assimilabile ad una operazione di *backup*.
  In generale questa funzione può non essere disponibile con le smartcard fornite dai Certificatori accreditati.
- **Export -** consente di esportare su un file in formato PKCS#12 una coppia di chiavi da utilizzare per la cifratura dei documenti (si noti che l'esportazione di una chiave privata per la firma digitale sarebbe del tutto illegale). Lo scopo di questa operazione è quello di eseguire un backup (definito *key recovery*)al fine di non perdere la possibilità di decifrare documenti crittografati in caso di perdita o distruzione del dispositivo di firma che contiene le relative chiavi.
  In generale questa funzione può non essere disponibile con le smartcard fornite dai Certificatori accreditati.
  NOTA: una coppia di chiavi di cifratura potrà essere esportata solo se è stata creata fin dall'inizio con l'opzione di key recovery.
- **Chiudi** - chiude la finestra di dialogo

4.8.11.1 Generazione di una coppia di chiavi

Viene mostrata una finestra di questo tipo:

L'utente deve scegliere la tipologia di utilizzo della coppia di chiavi ed agire su OK, per avviare il processo di generazione.

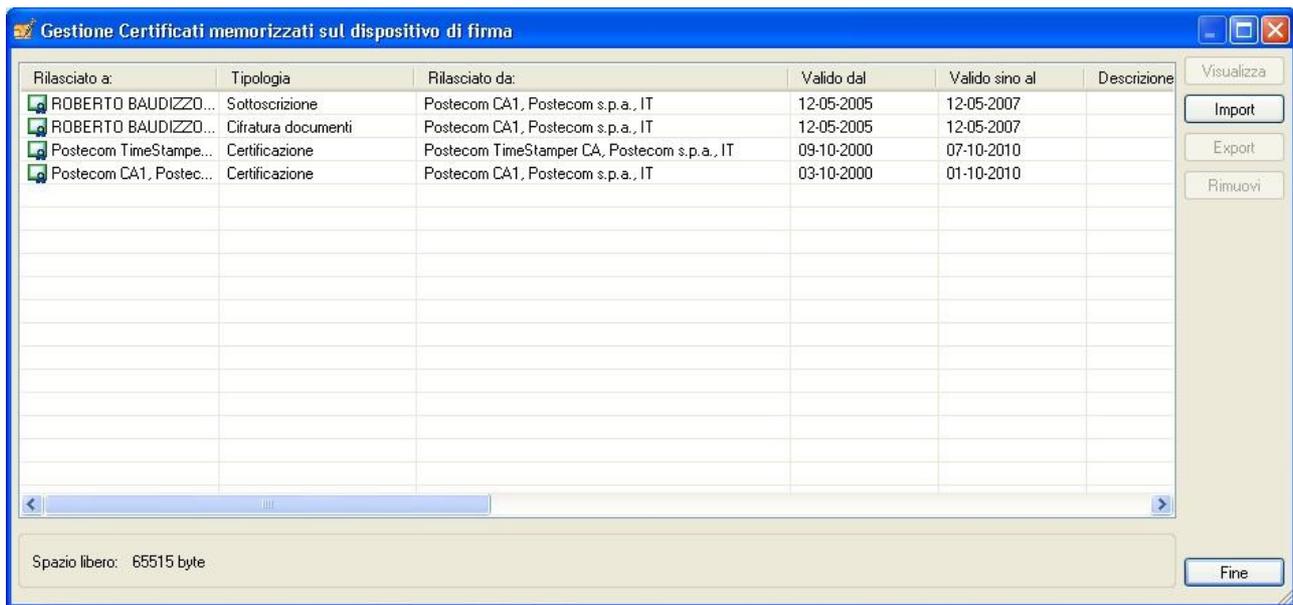
4.8.11.2 Proprietà di una coppia di chiavi

Viene mostrata una finestra di questo tipo:

La tabella della finestra mostra il certificato o i certificati presenti nel sistema e che corrispondono alla coppia di chiavi.

- il bottone **Aggiorna** ripete la scansione degli archivi di DigitalSign alla ricerca dei certificati
- **Visualizza** apre la visualizzazione del certificato selezionato
- **Export** consente di esportare su un file esterno una copia del certificato selezionato

4.8.12 Modulo di Gestione dei Certificati 'on-board'

Questo modulo consente di esplorare i certificati contenuti a bordo del dispositivo di firma correntemente inserito.

Sono disponibili i seguenti bottoni comando:

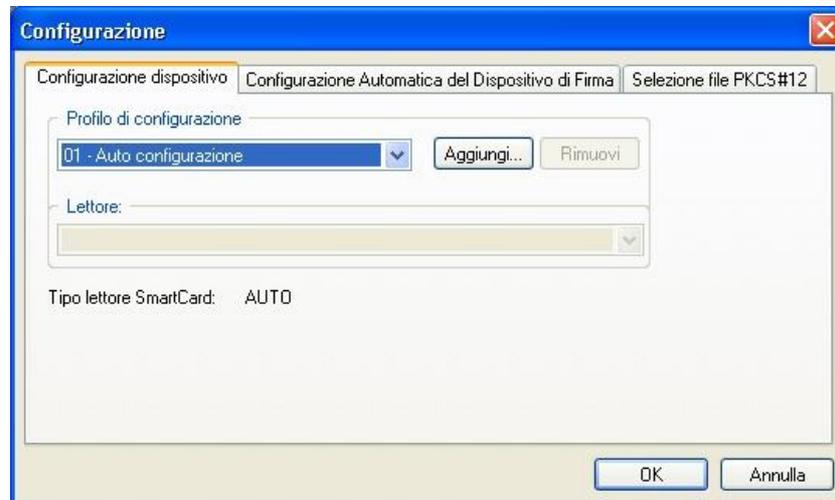
- **View** - per visualizzare il contenuto del certificato, tramite l'apposito visualizzatore (4.8.9)
- **Import** - per caricare nel dispositivo un certificato disponibile su file.
  L'effettiva disponibilità di questa funzione dipende dalla configurazione del particolare dispositivo
- **Export** - per esportare su un file esterno il certificato correntemente selezionato
- **Rimuovi** - per cancellare dalla memoria della smartcard il certificato selezionato.
  L'effettiva disponibilità di questa funzione dipende dalla configurazione del particolare dispositivo.
- **Annulla** - per chiudere la finestra di dialogo senza aggiornare la memoria del dispositivo con le modifiche eventualmente apportate (vedere NOTA in calce)
- **Salva su dispositivo** - per chiudere la finestra di dialogo, aggiornando effettivamente la memoria della smartcard (vedere NOTA in calce)

NOTA: Le funzioni attive di questo modulo (**Import**, **Rimuovi**) non agiscono direttamente sulla memoria del dispositivo di firma, ma su un buffer di memoria del computer.
Al termine delle operazioni il risultato si trasferisce effettivamente alla memoria del dispositivo con il comando **Salva su dispositivo**.

4.8.13 Modulo di Gestione della Configurazione del Dispositivo di Firma

DigitalSign può operare con una grande varietà di dispositivi di firma, che richiedono di essere correttamente interfacciati.
La gran parte delle smartcard e dei dispositivi di altro genere disponibili sul mercato – soprattutto quelli rilasciati dai Certificatori accreditati presso CNIPA – viene interfacciata attraverso lo standard PKCS#11, ma è possibile gestire alcuni dispositivi direttamente a livello APDU.
Nel primo caso DigitalSign deve mettere in funzione lo specifico modulo PKCS#11 (una .DLL) adatto per la particolare tipologia di smartcard, mentre nel secondo caso deve riconoscere correttamente il tipo di dispositivo ed attuare il corretto protocollo di comunicazione.

4.8.13.1 Auto-configurazione

Avendo a che fare con una smartcard già pronta all’uso, contenente chiavi e certificati, il modo più semplice di procedere è quello di attuare la configurazione automatica.

In questa modalità l’utente non deve fare nulla, ma solo lasciare che DigitalSign risolva automaticamente il problema della configurazione

Il sistema opera come segue:

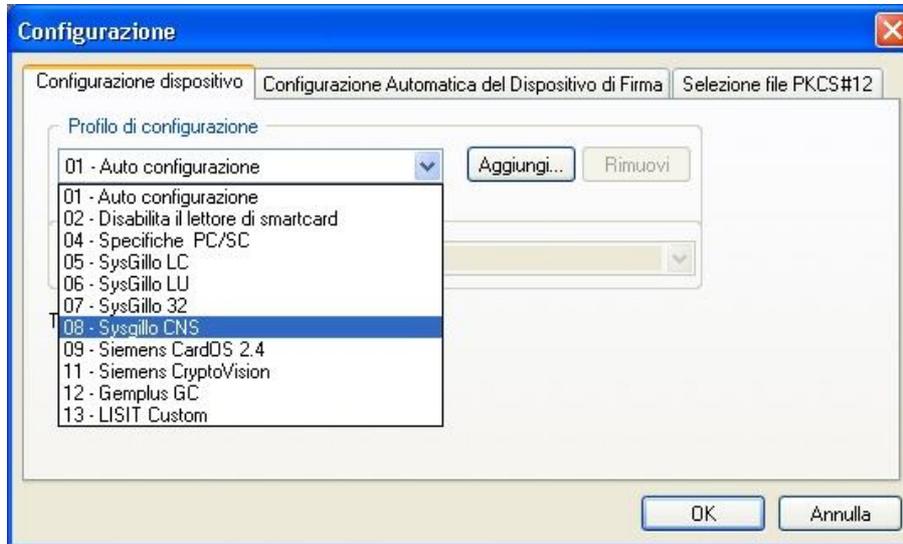
- all’avvio DigitalSign ricerca nel computer quali moduli PKCS#11 – tra quelli conosciuti da DigitalSign, elencati nel file **`devices.ini`** che si trova nella stessa cartella che ospita l’eseguibile – sono effettivamente presenti;
- al primo inserimento di una smartcard in uno dei lettori installati nel sistema DigitalSign tenta di leggerne i certificati contenuti in area pubblica (dove non è necessario disporre del PIN) attraverso i vari moduli PKCS#11 di cui dispone, fino a quando non ottiene un risultato positivo;
- una volta trovato il modulo PKCS#11 corretto DigitalSign registra l’associazione tra il codice identificativo del particolare tipo di smartcard (ATR) ed il modulo PKCS#11 che ha avuto successo nella lettura della carta, così da metterlo direttamente in uso la prossima volta che un dispositivo dello stesso tipo viene inserito in un lettore

Il funzionamento del processo di configurazione automatica può essere seguito visivamente dalla cartella **Configurazione Automatica del Dispositivo di Firma** disponibile nell’ambito di questo stesso modulo.

Come si può intuire questa strategia può non andare a buon fine, oltre all’ovvio caso in cui la macchina non disponga del giusto modulo PKCS#11, nel caso in cui l’area pubblica del dispositivo non contenga alcun certificato.
Questo si verifica con le carte interamente vuote o con alcune smartcard i cui certificati sono memorizzati tutti in area privata invece che in area pubblica (ad oggi abbiamo esperienza di alcuni dispositivi di questo tipo rilasciati da Actalis), per i quali è richiesta la configurazione manuale.

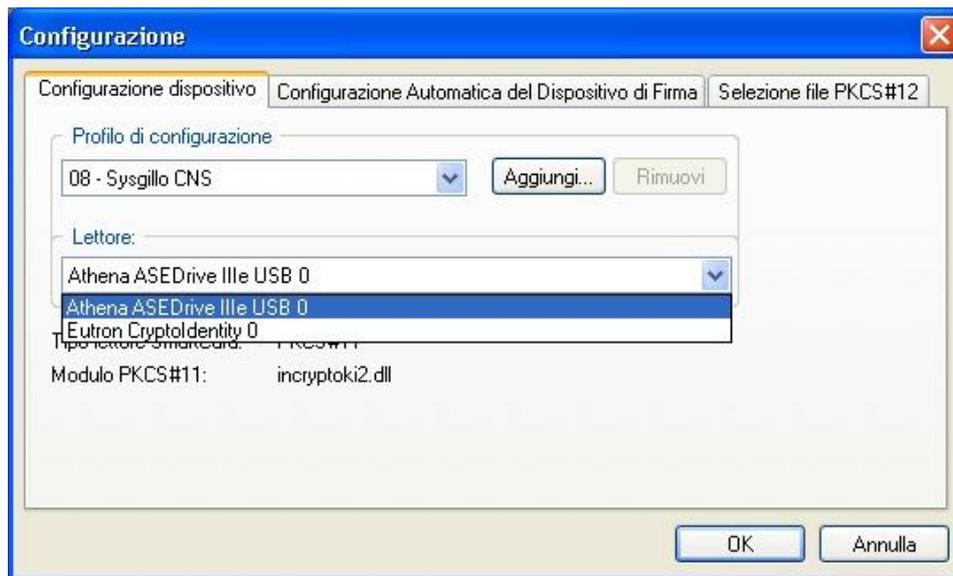
4.8.13.2 Configurazione manuale

Se il modulo di configurazione automatica non riesce ad associare correttamente la smartcard a disposizione con un modulo PKCS#11 tra quelli installati nel sistema (può essere il caso di

dispositivi vergini oppure di smartcard prive di certificati in area pubblica) è possibile eseguire la configurazione manuale, forzando DigitalSign a colloquiare con il dispositivo utilizzando una modalità ben determinata ed uno specifico lettore.

Innanzitutto occorre scegliere il modulo da impiegare, dalla lista completa di tutte le opzioni (in questa fase DigitalSign non ha ancora escluso i moduli non effettivamente installati sulla macchina).

Si noti che i primi elementi della lista sono speciali:

- 01 – **Auto configurazione** – attiva il riconoscimento automatico
- 02 – **Disabilita il lettore di smartcard** – predispone DigitalSign ad operare senza dispositivo di firma, evitando i messaggi di errore relativi all’assenza di un lettore
- 04 – **Specifiche PC/SC** – predispone DigitalSign ad interfacciare la smartcard in modalità APDU, senza alcuna intermediazione di moduli PKCS#11. In questa modalità sarà possibile utilizzare solo un set ristretto di dispositivi ben identificati

Dopo la selezione della modalità occorre anche specificare in quale lettore si trova il dispositivo, nel caso la macchina disponga di più di un lettore:

NOTA: l'esempio della figura mostra un lettore "virtuale", corrispondente ad un token USB che viene visto dal sistema come l'insieme lettore + smartcard. Dopo aver installato i relativi driver il lettore sembrerà sempre disponibile, ma se il token non è montato in una porta USB il lettore apparirà vuoto

Qualora il dispositivo a disposizione richiedesse, per l'interfacciamento, un modulo PKCS#11 diverso da tutti quelli noti a DigitalSign, è comunque possibile aggiungere un nuovo profilo tramite il bottone **Aggiungi**, si veda la prossima sezione.

4.8.13.3 Aggiunta di un Profilo di Configurazione

Questa finestra consente di registrare in DigitalSign un nuovo profilo di configurazione per dispositivi PKCS#11.

Occorre assegnare al profilo un nome simbolico ed indicare il file .DLL che rappresenta l'interfaccia PKCS#11.

I tre checkbox sottostanti hanno il seguente significato:

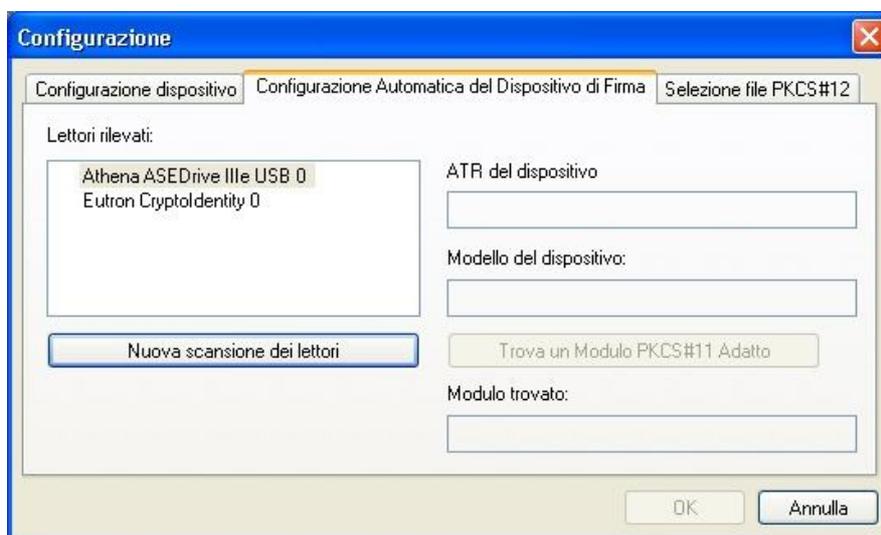
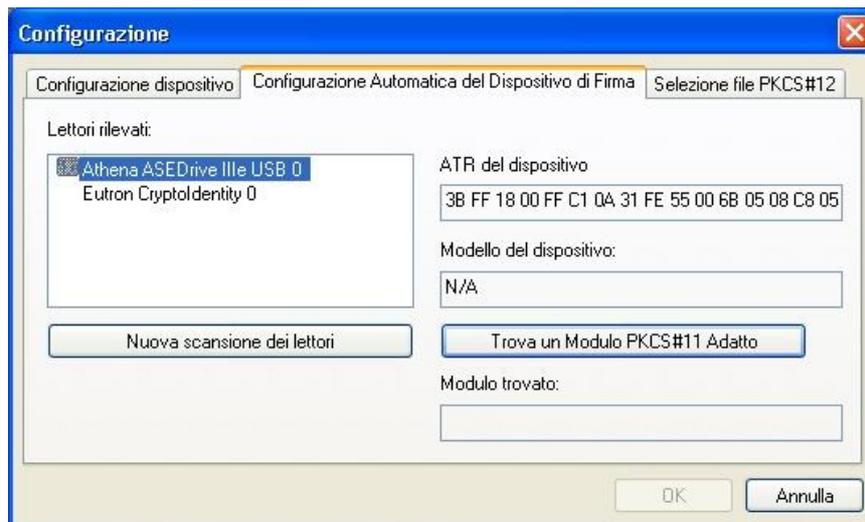
- **Attiva cache per il modulo PKCS#11** – se attivo fa sì che DigitalSign, una volta collegato positivamente un dispositivo a questo modulo, registri l'associazione mediante l'ATR del

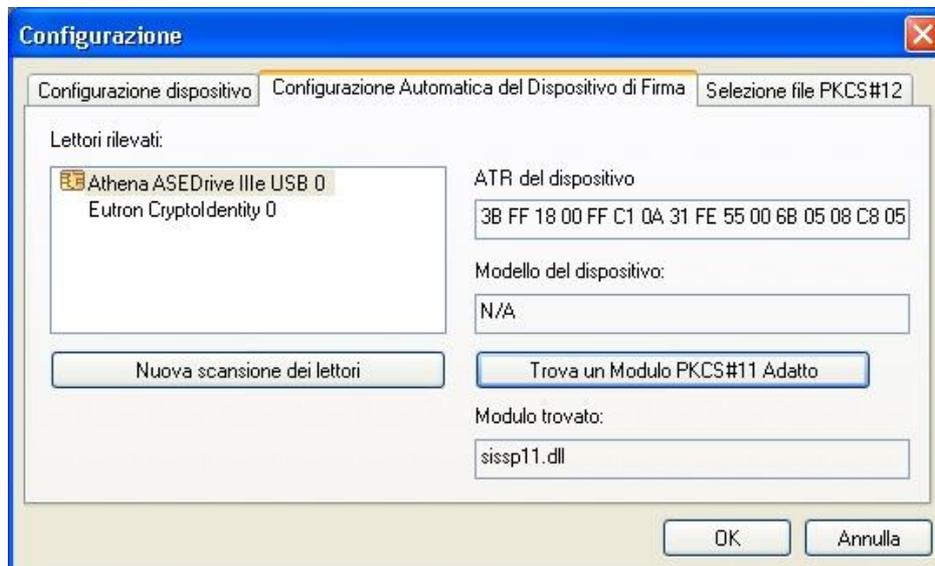
dispositivo stesso, così che successivi inserimenti di dispositivi dello stesso tipo colleghino direttamente questo modulo se è attiva la modalità di auto-configurazione.
In taluni casi può essere opportuno disabilitare questa opzione (per esempio con smartcard che hanno lo stesso ATR ma vengono personalizzati tramite diversi layer: è necessario lasciare che DigitalSign trovi il modulo giusto tramite la lettura sperimentale dei certificati di bordo)

- **Registra PIN callback** – questa è una funzione speciale, riservata ad uno specifico modulo (SISSP11) e consente di gestire in modo automatico il PIN di firma, evitando la doppia richiesta del PIN. Si raccomanda di non attivare questa opzione se non su indicazioni del fornitore
- **Abilita Attestazione** – questa opzione istruisce il sistema ad abilitare, per i dispositivi di firma interfacciati per tramite di questo modulo, la funzione di Attestazione (firma debole). In caso di abilitazione di questo checkbox è anche necessario specificare quale *“key usage”* devono avere i certificati da usare per questo scopo. Si raccomanda di usare **Digital Signature**.

4.8.13.4 Pannello di monitor del riconoscimento automatico

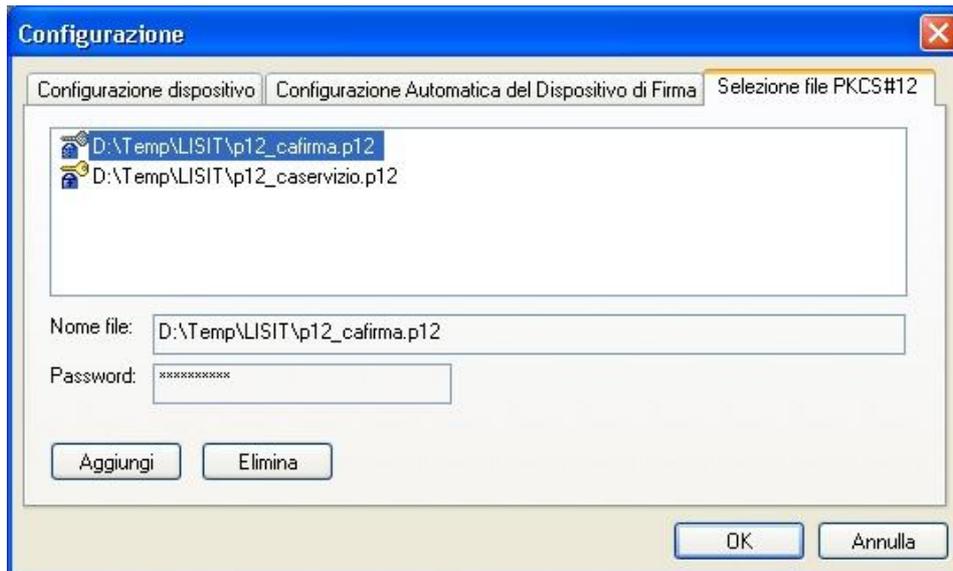
Questo pannello consente di controllare i passi svolti da DigitalSign nella ricerca automatica di un modulo PKCS#11 adatto ad interfacciare un dispositivo di firma.

Se nessun dispositivo è inserito in un lettore il pannello può presentarsi come in figura (in questo caso il sistema dispone di 2 lettori):

Il bottone **Nuova scansione dei lettori** forza il sistema a rileggere lo stato dei lettori, aggiornando la lista. Ma normalmente è sufficiente inserire una smartcard in un lettore per veder aggiornare la finestra in questo modo:

Il simbolo della smartcard appare accanto al nome del lettore, mentre nel riquadro a destra compare il codice ATR (*Answer To Reset*) del dispositivo.
Talvolta è disponibile anche una denominazione del modello del dispositivo.

Agendo sul bottone **Trova un modulo PKCS#11 adatto** si avvia il processo di tentativi illustrato in precedenza; se l'ATR del dispositivo in questione non era mai stato incontrato e se si dispone di diversi moduli li vedremo scorrere nell'edit box in basso con l'etichetta **Testing…**
Alla fine del procedimento la finestra si presenta come segue:

4.8.13.5 Caricamento file PKCS#12

Alcune funzioni di DigitalSign possono essere eseguite anche con chiavi RSA gestite in software, non residenti su smartcard; attualmente tale opzione è disponibile soltanto per le operazioni di decifratura documenti.
Se per le chiavi private di firma digitale è essenziale, a fini di sicurezza, che in nessun caso sia possibile l'esportazione o la duplicazione, per le chiavi private destinate alla decifratura di documenti è importante poter disporre del backup delle chiavi private.

Un documento cifrato diventa infatti del tutto illeggibile in caso di perdita o malfunzionamento della smartcard che contiene l’unica chiave privata idonea a decifrarlo. Quindi è prassi piuttosto comune usare per questo scopo delle chiavi private con opzione di key-recovery, che vengono esportate su file in formato PKCS#12 (sono file a loro volta cifrati e protetti con password, contenenti la chiave privata ed il relativo certificato).
Allorché si intende usare una chiave così esportata sarà possibile importarla su una nuova smartcard, ma è altresì possibile usarla direttamente dal file PKCS#12.

Questo modulo consente appunto l’utilizzo diretto di chiavi e certificati contenuti in file PKCS#12.

DigitalSign può caricare le chiavi ed i certificati di uno o più file PKCS#12 e gestirli come se fossero contenuti nella smartcard correntemente inserita.
A tal fine è necessario registrare i file PKCS#12 desiderati attraverso questo modulo, che presenta tutti i file correntemente registrati.

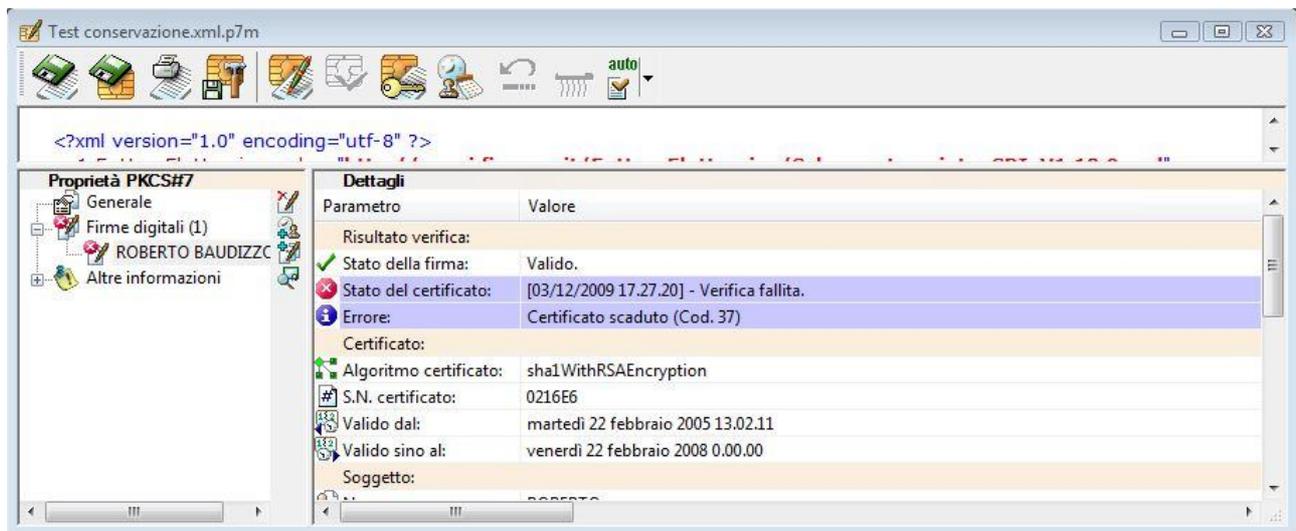
- Con il bottone **Elimina** si rimuove la registrazione del file correntemente selezionato
- Con il bottone **Aggiungi** si passa ad una ulteriore finestra:

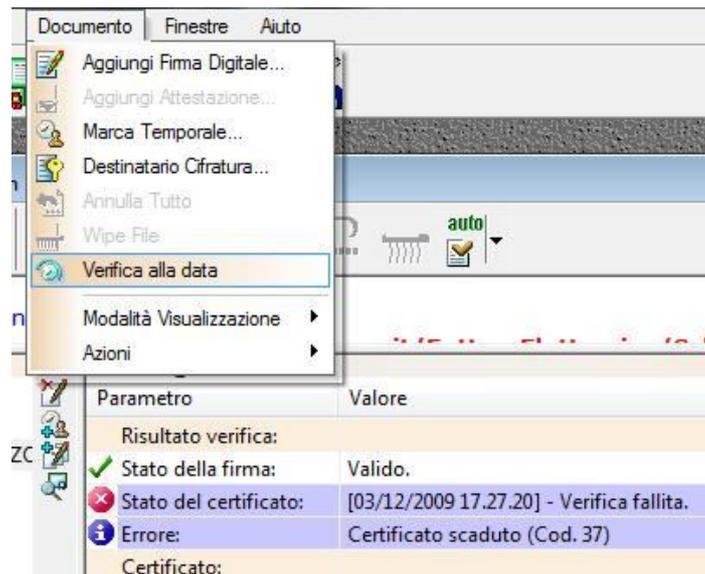
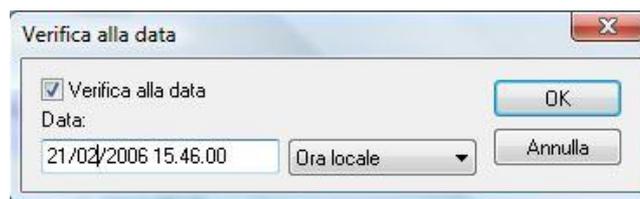
Da qui è possibile selezionare il file da importare e fornire la password per accedere al contenuto del file stesso.
Con **Import** si conferma la registrazione del file, con **Annulla** si torna alla schermata precedente.

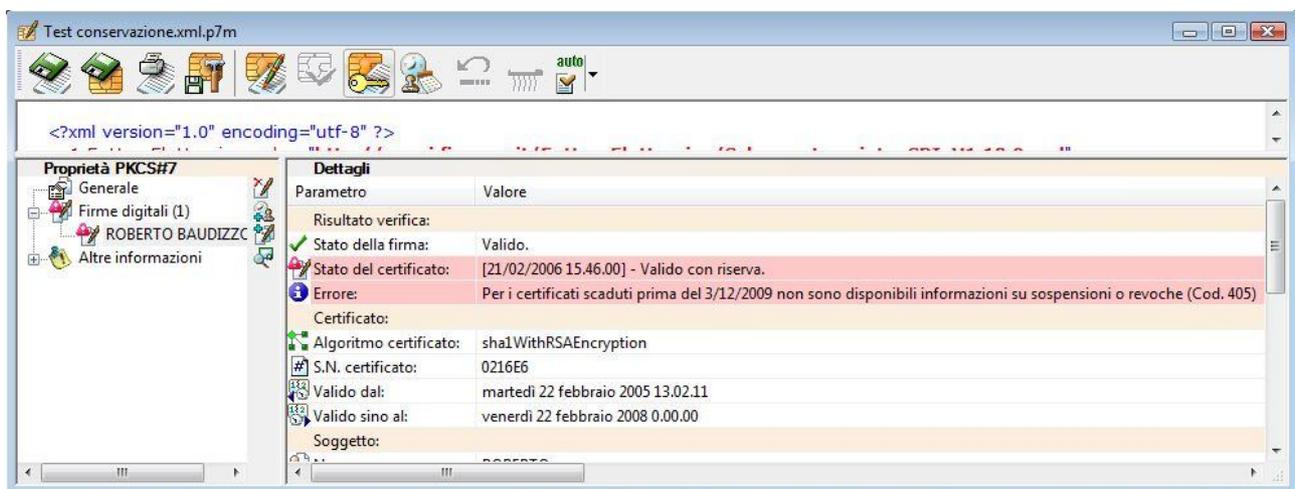
NOTA IMPORTANTE: si ribadisce che le chiavi ed i certificati importati dai file PKCS#12 specificati per tramite di questo ambiente di configurazione vengono utilizzati da DigitalSign – limitatamente alla funzione di decifratura documenti – come se le stesse chiavi e certificati fossero presenti nella smartcard correntemente inserita.
Questo significa anche che se nessuna smartcard è inserita, non sarà possibile usare nemmeno gli oggetti software letti dai file PKCS#12: questo perché l'architettura interna di DigitalSign mette in funzione certe strutture solo quando un dispositivo di firma è correttamente interfacciato.

4.8.14 Verifica alla Data

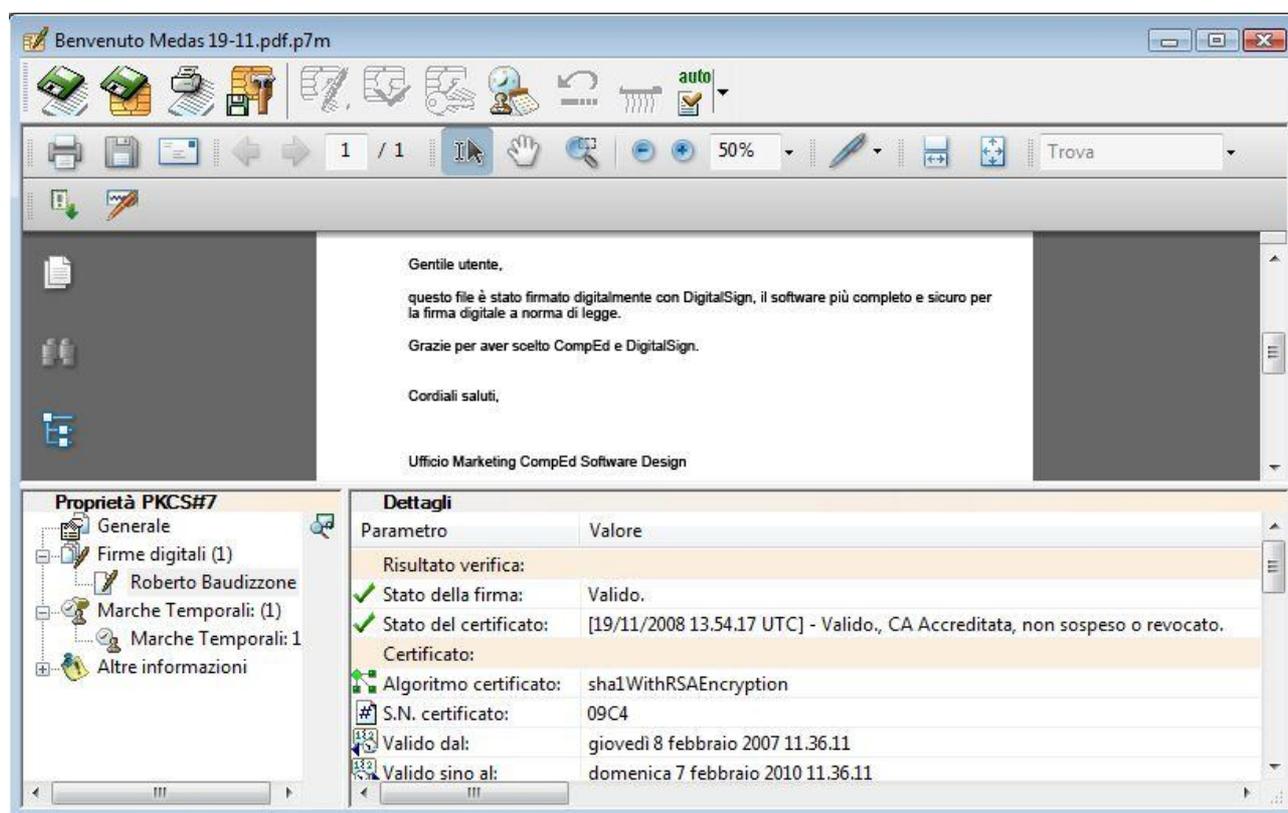
Con il 3 Dicembre 2009 è entrata in vigore una nuova modalità di emissione delle liste di sospensione e revoca (si veda la sezione sulla verifica delle firme digitali), che ora non vengono più depurate delle informazioni di revoca relativa a certificati di cui sia ormai terminata la validità nominale.
Grazie a questa novità è possibile, solo esaminando la CRL attuale, determinare se un certificato fosse indenne da provvedimenti di sospensione o revoca in una qualsiasi data compresa nel periodo di validità nominale (con l'esclusione di certificati comunque scaduti prima del 3/12/2009).
DigitalSign consente dunque di effettuare verifiche di firme digitali riferite ad una data qualsiasi, non quella attuale.

Normalmente, aprendo un documento firmato (non corredato di marca temporale) e navigando nel pannello delle proprietà sino ad espandere una particolare firma, vedremo qualcosa del genere:

Come si vede la riga relativa allo **Stato del Certificato** riporta tra parentesi quadre una data ed un'ora di riferimento (nella figura 3/12/2009, ore 17:27). In generale quella è la data ed ora attuale.
Nel caso in figura la verifica è "non superata" perché allo stato attuale il certificato risulta scaduto.

Se a questo punto vogliamo sapere se il certificato fosse valido in un'epoca passata possiamo utilizzare la funzione di **Verifica alla Data:**

Verrà visualizzata questa piccola finestra di dialogo:

L'utente sarà invitato a selezionare il checkbox per attivare la verifica ad una data diversa da quella attuale, quindi ad inserire la data ed ora di riferimento (eventualmente distinguendo, liberamente, tra ora locale e UTC). Nel nostro caso inseriremo una data anteriore a quella di scadenza del certificato in questione.

Una volta premuto OK DigitalSign aggiorna i propri pannelli e mostra il risultato della verifica ricalcolato alla data indicata dall'utente:

Questa immagine mostra un effetto particolare, che in quest'epoca sarà molto comune e tenderà poi a diventare più raro.
Come detto, le CRL contengono obbligatoriamente le informazioni di sospensioni e revoca anche per certificati ormai scaduti solo dal 3 dicembre 2009. Quindi, se il certificato in corso di analisi è scaduto prima di tale data e la CRL non contiene alcun riferimento a quel certificato, non è possibile stabilire con certezza che effettivamente non fosse mai avvenuta una sospensione o revoca. Quindi, in un caso del genere, DigitalSign dichiarerà "valido con riserva" e segnala un opportuno messaggio di warning.

4.8.14.1 Verifica di documenti marcati temporalmente

Il meccanismo di *Verifica alla Data* è particolarmente utile quando si verifichino documenti firmati e marcati temporalmente.
In questo caso DigitalSign esegue automaticamente la verifica riferita alla data ed ora corrispondenti alla marca temporale, presentando con un solo colpo d'occhio l'effettivo stato di validità di un documento marcato temporalmente:

Se andiamo poi ad aprire un documento marcato temporalmente tempo addietro, tanto che il relativo certificato (della marca temporale) sia già scaduto, vedremo che DigitalSign considera comunque valida la marca temporale tenendo conto del periodo di validità stabilito dalla normativa, in base alla configurazione delle opzioni di security, sezione firma e verifica:

4.9 Appendici

4.9.1 Modalità di interfacciamento dei dispositivi di firma

DigitalSign svolge molte delle sue funzioni più importanti basandosi sui servizi offerti da un dispositivo di firma (smartcard, token USB, HSM).
Poiché si tratta di dispositivi esterni devono essere interfacciati correttamente.
La varietà di dispositivi disponibili, naturalmente, rende l'obiettivo della compatibilità generalizzata più complesso.
In questa sezione si illustrano le differenze tra le due modalità di interfacciamento fondamentali.

4.9.1.1 Dispositivi interfacciati a livello PKCS#11

DigitalSign supporta dispositivi di firma compatibili con lo standard PKCS#11.

Questo significa che DigitalSign, quando opera in questa modalità (invece che tramite interfacciamento a livello APDU), si interfaccia solo a livello software con un modulo standard PKCS#11 reso disponibile dal fornitore del dispositivo stesso.
In questo modo DigitalSign non deve "conoscere" i dettagli fisici del dispositivo, che vengono gestiti dal modulo di interfaccia.

Quando DigitalSign opera con dispositivi di firma rilasciati da un certificatore accreditato presso CNIPA si tratta sempre di dispositivi PKCS#11.

Un modulo PKCS#11 fisicamente consiste di una DLL al quale DigitalSign deve collegarsi per interagire con il dispositivo.

L'utente deve verificare i requisiti di sistema (sistema operativo e risorse in primo luogo) specificati dal produttore e la loro compatibilità con quelli di DigitalSign; inoltre deve verificare se il modulo PKCS#11 richiede un particolare tipo di lettore di smartcard o altri componenti hardware/software installati o configurati.

CompEd conduce un continuo lavoro di aggiornamento del software e dei profili di configurazione per consentire l'utilizzo dei dispositivi presenti sul mercato. All'utente è normalmente sufficiente:

- assicurarsi di aver installato sul sistema il software PKCS#11 adatto alla smartcard o al dispositivo in proprio possesso
- lasciare che il modulo di riconoscimento automatico riconosca da sé il dispositivo

La tabella che segue illustra i dispositivi testati con DigitalSign. Si vedano con attenzione anche le NOTE che seguono la tabella.

Dispositivo	Modulo PKCS#11	Modulo DigitalSign (1)	Certificatori (2)	Note
Smartcard Gemplus GemGATE 32K	GemPKCS 4.6.006 gclib.dll (v. 4.5.5.1)	Gemplus GC	Actalis, Postecom	
Smartcard Siemens CardOSM4.01/a	CardOS 2.4.0 si_pkcs11.dll (v. 2.0.21.14)	Siemens Cardos 2.4	Actalis, Infocamere, IT-Telecom, Postecom	(3)
Smartcard Incard CS16	Sysgillo 1.9.10.0 ipmpkiLC.dll (v. 1.0.1.0) o ipmpki32.dll (v. 1.9.10.0)	Sysgillo LC o Sysgillo 32	Infocamere IT-Telecom	
Smartcard Incard CSE4H	Sysgillo 1.9.10.0 ipmpkiLC.dll (v. 1.0.1.0) o ipmpkiLU.dll (v. 1.9.10.0)	Sysgillo LC o Sysgillo LU	Infocamere IT-Telecom	
Smartcard Cryptovision	Cryptovision cv_p11_M4.dll (v. 2.2.0.0)	Siemens Cryptovision	Infocamere	
Token USB Eutron CryptoIdentity (n.serie 1501…)	Siemens CardOS 2.4.0 si_pkcs11.dll (v. 2.0.21.14)	Siemens Cardos 2.4	Actalis, Infocamere, IT-Telecom	(4)
Smartcard CNS Incard Incrypto34V2 (n.serie 7420…, 1204…)	Sysgillo 2.3 incryptoki2.dll (v. 2.5.1.6 o v. 2.4.9.3)	Sysgillo CNS	Actalis, Infocamere, Infocert, Postecom	(5)
Smartcard Siemens SISS HPC	SISS API 0.0.5 SissP11.dll (v. 2.0.23.0)	SISS	LISIT	(6)
Token USB “Business-Key”	Sysgillo 2.3 incryptoki2.dll (v. 2.5.1.6 o v. 2.4.9.3)	Sysgillo CNS	Infocert	(7)
Smartcard CNS Oberthur	Bit4Id bit4opki.dll (v. 1.1.4.6)	Oberthur CNS	Actalis	(8)
Smartcard Charismatics	Charismatics cmp11.dll (v. 3.2.2.4)	Charismatics SI	Actalis	

NOTE:

(1) La colonna “Modulo DigitalSign” indica il nome simbolico del profilo di dispositivo utilizzato da DigitalSign per interfacciare il dispositivo.
Tali nomi sono indicati tramite il file devices.ini, che associa il nome di ogni profilo ad una specifica DLL di interfaccia.
Poiché i nomi dei profili possono cambiare nel tempo per varie ragioni, si precisa che i nomi contenuti nella tabella sono riferiti ai profili definiti con la versione 3.0.3.11 di DigitalSign e successive.

(2) La colonna “Certificatori” indica i certificatori iscritti all’elenco CNIPA dei Certificatori Accreditati che risulta abbiano distribuito dispositivi nelle varie tecnologie. Il contenuto della colonna è del tutto indicativo.

(3) Esistono in circolazione alcune tipologie di smartcard di questa tecnologia che non contengono il certificato qualificato dell’utente nell’area pubblica. Quindi non possono essere riconosciute dalla modalità “riconoscimento automatico” di DigitalSign, che si basa appunto sull’esito della lettura del certificato.
Occorre impostare manualmente il modulo indicato ed effettuare il logon per accedere al certificato ed ai servizi.
Questa limitazione è stata osservata in dispositivi rilasciati da Actalis.

(4) Oltre all'installazione del modulo PKCS#11 è necessario installare anche i driver specifici che emulano un lettore di smartcard

(5) Queste smartcard, definite "Carta Nazionale dei Servizi con dispositivo di firma digitale", hanno una particolare struttura interna organizzata in diverse sezioni. In particolare la parte dedicata alla firma digitale è distinta dalla parte contenente chiavi di autenticazione ed è previsto che si usino due diversi codici PIN per le due diverse sezioni.
Questa flessibilità presenta tuttavia uno svantaggio per le applicazioni di firma digitale, perché il software di interfaccia PKCS#11 (SysGillo) potrebbe richiedere di propria iniziativa la nuova digitazione del PIN anche se la carta già si trova in stato di LogOn. Questo effetto risulta particolarmente sgradevole in caso di procedure di firma automatica, per firmare lotti di documenti in unica soluzione.
Allo stato siamo a conoscenza di tre diversi moduli PKCS#11 in grado di interfacciare queste smartcard:
- SysGillo 2.3 standard (con incrlyptoki2.dll v. 2.4.9.3), richiede doppia digitazione del PIN
- SysGillo 2.3 MODIFICATO (con incryptoki2.dll v. 2.4.9.3), NON richiede doppia digitazione del PIN
- componenti installati dal software Dike di Infocamere (con incryptoki2.dll v. 2.5.1.6), consente scelta della digitazione singola o doppia del PIN dal menu di Dike.

(6) Queste smartcard sono delle CNS (Carta Nazionale dei Servizi) distribuite dalla Regione Lombardia e richiedono uno specifico modulo di interfaccia PKCS#11 (vedere tabella). Anche queste carte, come quelle descritte al punto precedente, richiedono una digitazione del PIN subito prima di ogni firma anche se la carta già si trova in stato di LogOn. A partire dalla versione 3.0.3.13 DigiitalSign contiene un modulo *callback* specifico, realizzato sulle specifiche del produttore del software PKCS#11, che permette di aggirare questo problema se il PIN utente ed il PIN firma sono uguali. Se tali PIN sono diversi il modulo callback rischia di bloccare la smartcard.
Per tale ragione questo modulo *callback* va espressamente abilitato intervenendo sul file **`devices.ini`**.

(7) Questi dispositivi sono dotati di memoria flash e di un dedicato software di virtualizzazione che consente di spostare il dispositivo da un computer all'altro senza richiedere installazione. Tuttavia questa possibilità è limitata all'uso del software a corredo.
Se si desidera utilizzarli con DigitalSign installato sul computer è necessario che il modulo PKCS#11 sia installato sul computer.

(8) Queste smartcard sono CNS e come tali presentano il problema della doppia digitazione del PIN descritta più sopra a proposito di altre CNS. Tuttavia è possibile configurare il modulo PKCS#11 in modo da evitare la doppia richiesta, si consulti la documentazione di Bit4Id.
Per questi dispositivi, testati in preserie, sono stati osservati tempi di risposta straordinariamente lenti.

Si noti che l'elenco dei Certificatori operativi è in continua evoluzione; ovviamente ogni Certificatore è libero di adottare diversi tipi di dispositivi e di adottare/fornire diversi software di interfaccia PKCS#11; inoltre i diversi Certificatori attuano diverse politiche di distribuzione del software PKCS#11 che permetterebbe al titolare di una smartcard di utilizzare il proprio dispositivo con il software applicativo di propria scelta.

Anche per tutte queste ragioni l'effettiva operatività di un particolare dispositivo con DigitalSign non può essere garantita a priori e va verificata a cura dell'utente.
Tuttavia CompEd pone continuamente in atto il massimo impegno affinché DigitalSign funzioni senza problemi con tutti i dispositivi disponibili sul mercato. La tabella della pagina precedente rappresenta il risultato delle osservazioni di CompEd nelle più tipiche condizioni di utilizzo.

Si vuole ribadire che l'utilizzo di un dispositivo PKCS#11 avviene mediante l'interfacciamento di un modulo software distribuito dal soggetto che distribuisce la smartcard (di regola il Certificatore); tale software non è di produzione CompEd; la compatibilità di tale software con l'hardware e l'ambiente operativo dell'utente non è competenza di CompEd. La tabella si limita ad indicare che in normali condizioni è stato possibile interfacciare ed utilizzare il dispositivo per le operazioni usuali (Logon, generazione firma, cifratura ove disponibile un certificato compatibile). I test sono stati effettuati con diversi lettori e con sistema operativo Windows XP.
Non è possibile senza escludere che un modulo possa essere compatibile anche con condizioni differenti, né che possa essere incompatibile con condizioni analoghe riprodotte in altri contesti.

4.9.1.2 Dispositivi interfacciati a livello APDU

APDU significa *Application Protocol Data Uni*t.

Un dispositivo di firma del tipo di una smartcard comunica con l'esterno attraverso un protocollo specifico, utilizzando un proprio set di comandi ed istruzioni (le APDU, appunto), richiedendo particolari strategie operative.

Esistono diversi chip (hardware) utilizzati nelle smartcard, diversi sistemi operativi installati sui dispositivi, diverse versioni. Evidentemente ogni combinazione di questi elementi richiede un interfacciamento specifico.

DigitalSign contiene diversi moduli di interfaccia per altrettante famiglie di smartcard, riuscendo a controllare questi dispositivi senza l'intermediazione di un modulo PKCS#11 (quindi in modo più efficiente e flessibile).

Purtroppo non è possibile interagire in questo modo con una smartcard se questa è già stata inizializzata e personalizzata da un certificatore attraverso un layer PKCS#11 (cioè la totalità dei certificatori operanti attualmente in Italia), quindi la modalità APDU è oggi riservata ad applicazioni basate su certificati prodotti tramite la Personal Certification Authority.

Segue una tabella di dispositivi supportati in questa modalità:

Dispositivo	Produttore	Modello	Codice ATR (1)
Smartcard	Schlumberger	Cryptoflex 8K	3B, 85, 40, 20, 68, 01, 01, 03, 05
			3B, 85, 40, 20, 68, 01, 01, 05, 01
			3B, 95, 15, 40, FF, 68, 01, 02, 01, 01
			3B, 95, 15, 40, FF, 68, 01, 02, 02, 01
			3B, 95, 15, 40, FF, 68, 01, 02, 02, 04
	Gemplus	GPK8000su512	3B, A7, 00, 40, 18, 80, 65, A2, 08, 01, 01, 52
	Siemens (1)	CardOS M4	3B, E2, 00, FF, C1, 10, 31, FE, 55, C8, 02, 9C
			3B, F2, 98, 00, FF, C1, 10, 31, FE, 55, C8, 03, 15
			3B, F2, 98, 00, FF, C1, 10, 31, FE, 55, C8, 04, 12

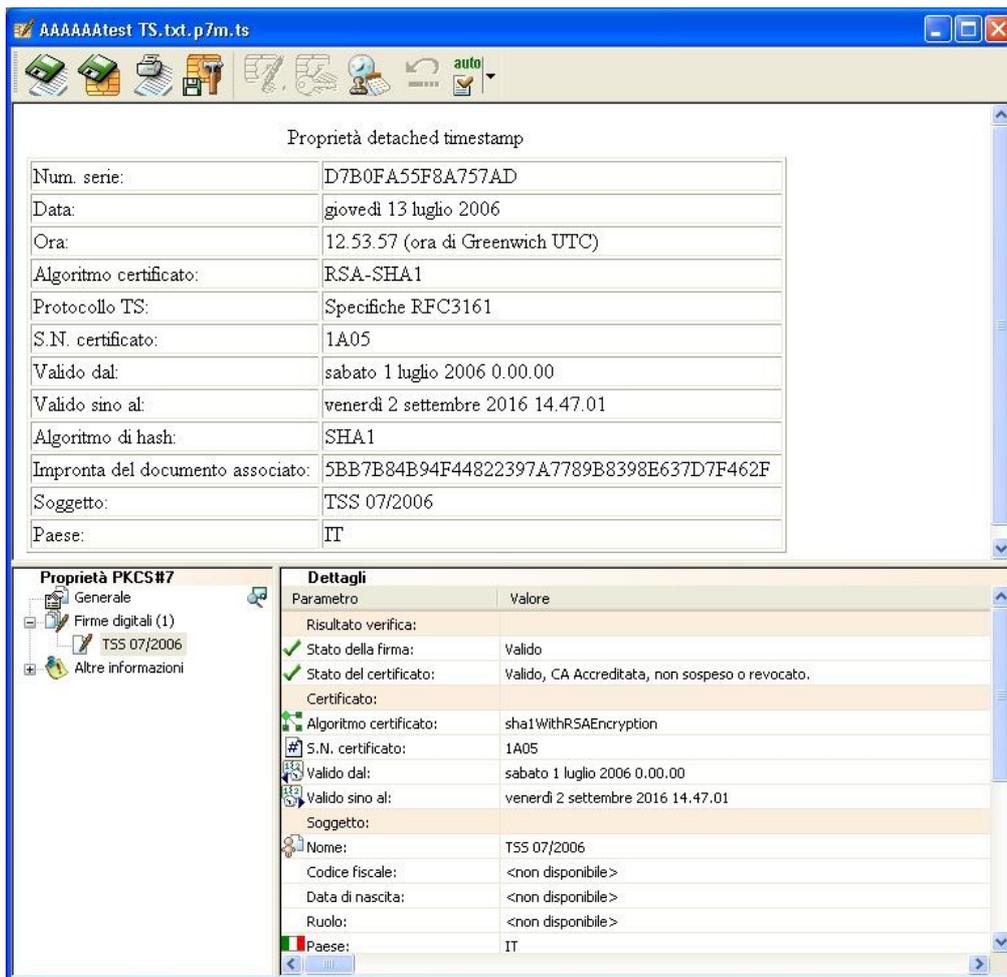
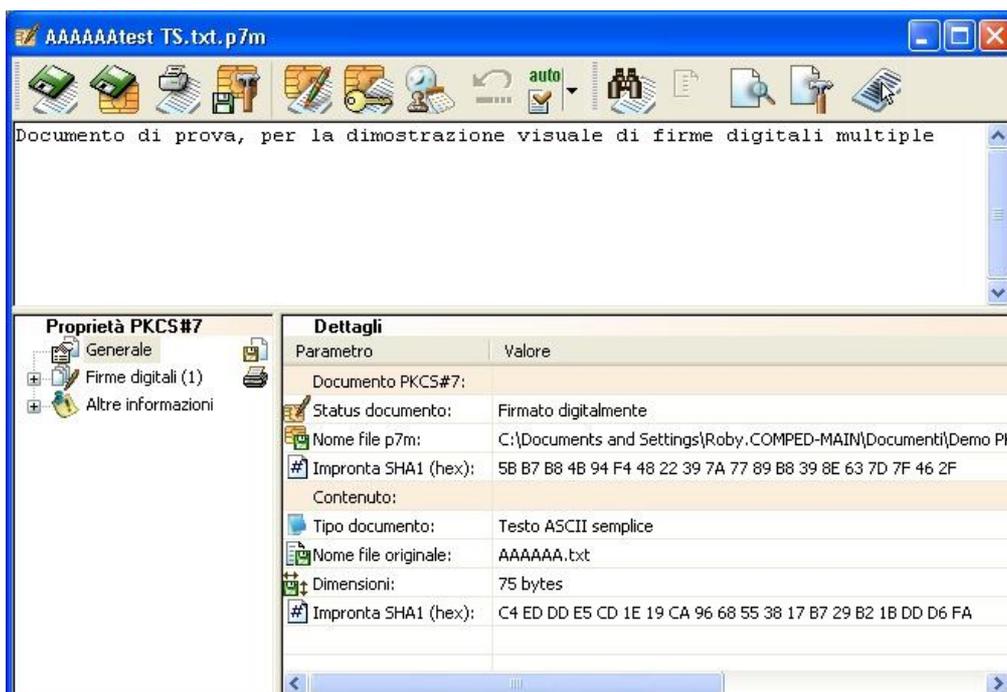
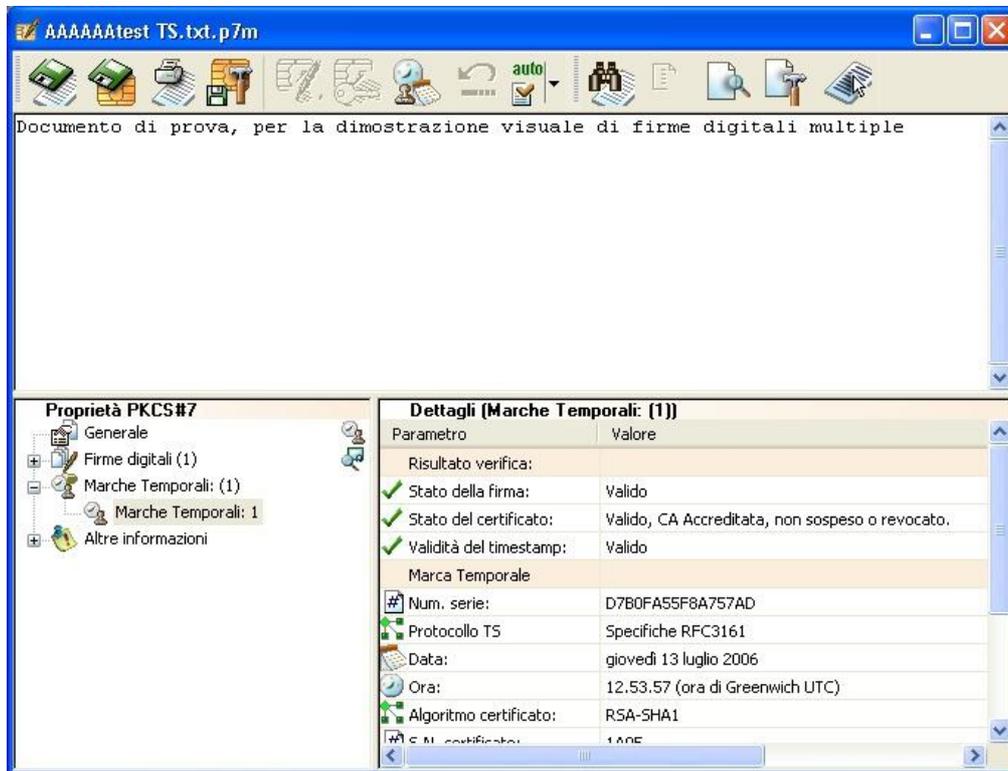
NOTA (1): il supporto di queste smartcard è disabilitato per default. Per abilitarlo è necessario inserire nel file <*nome eseguibile*>.INI:

```
[ low_level_sc_support ]
EnableCardOS=Y
```

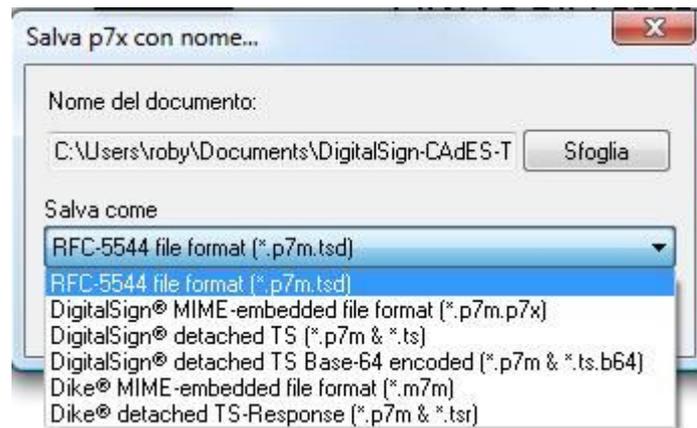
4.9.2 Marche temporali: contenuto e modalità di associazione ai documenti

Una marca temporale è di per sé un documento informatico firmato digitalmente.
I fornitori del Servizio di Marcatura Temporale accreditati presso DigitPA erogano tali marche temporali in accordo con le specifiche descritte nella Deliberazione CNIPA 45/2009.
Il formato del documento che rappresenta la marca temporale è il PKCS#7.

Non va però dimenticato che una marca temporale ha poco significato di per sé, mentre è fondamentale il suo significato quando è associata ad un altro documento informatico: poiché la marca temporale contiene l’impronta del documento a cui è associata serve a dimostrare l’esistenza di tale documento all’istante testimoniato dalla marca temporale.

La figura qui sotto mostra il contenuto di una marca temporale esaminata separatamente dal documento cui è riferita:

Quest’altra mostra il documento a cui la marca era stata associata. Si noti la coincidenza dei valori di impronta:

Naturalmente sarebbe troppo macchinoso per l'utente verificare visivamente l'identità dell'impronta del documento e quello dell'impronta oggetto della marca temporale; per questo DigitalSign apre la coppia di documenti insieme, mostrando il documento marcato temporalmente:

Ma per ottenere un tale obiettivo occorre individuare una modalità per associare i due oggetti. Le regole tecniche contenute nella Deliberazione CNIPA 45/2009 finalmente individuano un formato standard (RFC 5544) per associare un documento ad una marca temporale ed indicano anche una modalità per associare direttamente una marca temporale ad una firma (CAdES-T).

La seconda modalità è "trasparente" rispetto alla necessità di memorizzazione, perché la marca temporale è integrate nella busta crittografica .p7m.

La prima modalità, invece, prevede che si produca un file .tsd che incorpora i due oggetti originariamente separati (documento e marca).
Allo stato DigitalSign consente ancora di salvare i documenti marcati temporalmente nei formati proprietari utilizzati fino allentata in vigore della Deliberazione CNIPA 45/2009 (Settembre 2010), ma si raccomanda senz'altro di utilizzare il nuovo formato.

Le diverse modalità supportate sono le seguenti:

- **Modalità “RFC-5544 file format (*.p7m.tsd)**
  È lo standard previsto dalle regole tecniche 2009 per rappresentare un documento firmato (CAdES-BES) ed una marca temporale detached che copra lintero documento.

- **Modalità "DigitalSign MIME-embedded file format (*.p7m.p7x)"**
  Compatibilità: uso non raccomandato
  Per facilitare la manipolazione di documenti marcati temporalmente questa modalità prevede di raggruppare i due oggetti PKCS#7 in un unico file.
  Per ottenere tale scopo si adotta una struttura MIME, così da consentire una agevole separazione dei due oggetti con strumenti convenzionali, anche senza l'utilizzo di DigitalSign.

- **Modalità "DigitalSign detached TS (*.p7m & *ts)"**
  Compatibilità: uso non raccomandato
  Il documento e la marca temporale vengono memorizzati separatamente, come due file PKCS#7 codificati in DER.
  La *naming convention* adottata prevede per il documento vero e proprio la denominazione prescritta da AIPA/CNIPA (es. mydoc.pdf.p7m) e per la marca temporale lo stesso nome con l'ulteriore estensione .ts (es. mydoc.pdf.p7m.ts).
  Poiché i due file hanno lo stesso nome DigitalSign trova immediatamente la marca temporale al momento di aprire il file principale (ovviamente a condizione che i due file siano memorizzati nella stessa cartella.

- **Modalità "DigitalSign detached TS Base-64 encoded (*.p7m & *ts.b64)"**
  Compatibilità: uso non raccomandato
  Del tutto analoga alla modalità precedente, ma entrambi i file sono espressi in formato base64. La marca temporale reca l'estensione specifica (per chiarezza), mentre il documento mantiene l'estensione .p7m in ossequio alle linee guida di CNIPA.

- **Modalità "Dike MIME-embedded file format (*.m7m)"**
  Compatibilità: uso non raccomandato
  Questa modalità, introdotta in seguito da Infocamere con il proprio prodotto Dike ®, è molto simile a quella attuata nel formato .p7x di DigitalSign, ma diversa nel formato.
  Si tratta di una struttura MIME il cui contenuto è però codificato in binario e non in base64.

- **Modalità "Dike detached TS-Response (.p7m & *.tsr)"**
  Compatibilità: uso non raccomandato
  Anche questo formato è stato introdotto da Infocamere e rappresenta una sorta di ibrido tra le due modalità "detached" originariamente previste in DigitalSign: il documento è codificato in binario DER, mentre la marca temporale è in base64. Inoltre viene usata un'estensione particolare (.tsr) per il file della marca temporale separata.

Segue una tabella con i servizi di marcatura temporale testati positivamente con DigitalSign:

Provider	Servizio	Indirizzo Internet	Note
Actalis	Actalis TSA	https://193.203.230.233/test/proxy/proxyTSA.php	
Infocamere	Infocamere TSA	https://www.carm.infocamere.it/carm.dts/ServletDTS	
IT-Telecom	IT Telecom FirmaSicura	https://portal.tipki.it/tsservicesslminint/servletts	Policy: 1.3.76.12.1.1.2
IT-Telecom	IT Telecom MDI	https://portal.tipki.it/tsservicesslminint/servletts	Policy: 1.3.76.12.1.1.2
LISIT	CRS-SISS-TSA	(da richiedere al Provider)	
Intesa	Intesa-TSA	(da richiedere al Provider)	
ArubaPEC	ArubaPEC-TSA	(da richiedere al Provider)	

4.9.3 La cifratura dei contenuti in DigitalSign

La cifratura del contenuto di un documento, in DigitalSign, avviene direttamente all'interno di una struttura PKCS#7 e può riguardare documenti firmati o privi di firma (ovviamente, nel caso di documenti firmati, la firma viene calcolata sul documento in chiaro, prima della cifratura).

L'algoritmo di cifratura è di tipo misto:

- innanzitutto viene generata, con una procedimento casuale, una chiave di crittografia simmetrica
- la chiave simmetrica viene usata per cifrare il contenuto del documento
- la stessa chiave simmetrica viene poi cifrata a sua volta usando la chiave pubblica del destinatario; nel caso siano previsti più destinatari questa operazione viene ripetuta per ciascuno di essi. La chiave pubblica di ogni destinatario viene estratta dal relativo certificato (si ricorda che la selezione dei destinatari di cifratura avviene selezionandone i relativi certificati)
- il documento viene confezionato inserendo nella busta PKCS#7 il documento cifrato e tutte le copie cifrate della chiave simmetrica

Il destinatario potrà usare la propria chiave privata per decifrare la chiave simmetrica e quindi potrà usare quest'ultima per decodificare il documento.

NOTA: la crittografia simmetrica è basata sull'algoritmo selezionato a livello di opzioni tra una lista molto nutrita di alternative. La funzione predefinita (des-ede3-cbc a 192 bit) è estremamente robusta, praticamente inviolabile.

La crittografia asimmetrica attuata sulla chiave simmetrica viene invece eseguita con l'algoritmo supportato dalla chiave pubblica disponibile. Di norma è RSA a 1024 bit, ma certe smartcard supportano per questo scopo solo chiavi di lunghezza inferiore, nel qual caso la robustezza globale ne risulta diminuita.

4.9.4 Integrazione di DigitalSign 3.0 con altri prodotti software di produttività individuale

La seguente tabella mostra l'integrazione di DigitalSign 3.0 con alcuni prodotti software utilizzati per visualizzare i documenti da firmare. In particolare la tabella riporta, per ciascun prodotto: le versioni collaudate, i formati dei documenti generati, i riferimenti per i formati che sono standard internazionali e un'indicazione del livello di sicurezza associato all'operazione di firma effettuata visualizzando il documento da firmare con tale software.

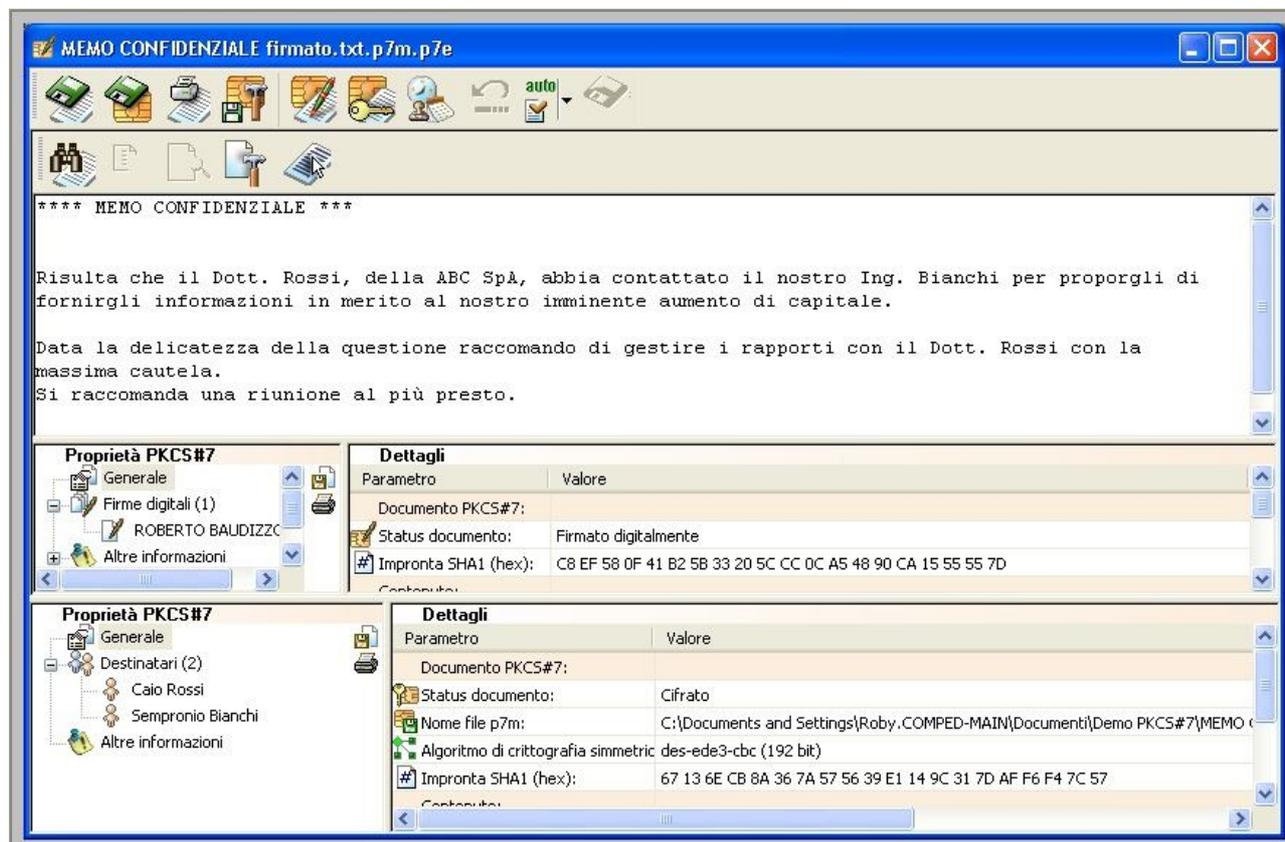
Software utilizzato da DigitalSign 3.0 per la visualizzazione dei documenti (1)	Versione	Formato file	Standard ISO e Publicly Available Specification	Livello di sicurezza (2)
CompEd SecurView	3.0	JPG, TIF, WMF, BMP, PCX, PSD, PNG, TGA, EPS, CMP, TXT, RTF, XML (3), binario (present. HEX)	JPG (ISO/IEC 10918-4:1999) TIF (ISO 12639:1998) BMP, WMF (www.microsoft.com) PSD, CMP (www.adobe.com) PNG (www.libpng.org/pub/png) TGA (Truevision Inc. Indianapolis)	*****
Adobe Acrobat	4.0, 5.0, 6.0, 7.0	PDF		**** (*** Adobe 7.0)
Adobe Acrobat Reader	4.0, 5.0, 6.0, 7.0	PDF		
Microsoft Internet Explorer	4.01 o sup.	HTML, XML (3)	HTML (www.w3.org)	
Microsoft Word	97, 2000, XP, 2003	DOC		***
Microsoft Excel	97, 2000, XP, 2003	XLS		
Microsoft PowerPoint	97, 2000, XP, 2003	PPT		
Altri prodotti sw compatibili con Microsoft Active Document	--	--		
Altre applicazioni esterne installate sul PC				*

Note:
(1) Ad eccezione di SecurView di CompEd, i prodotti software sopra indicati non sono inclusi in DigitalSign
(2) Il livello di sicurezza è maggiore al crescere del numero di "*" indicati in tabella. I valori riportati hanno carattere indicativo, relativo al tipo di tecnologia utilizzato.
(3) Il formato XML viene presentato per mezzo di Internet Explorer – al di sotto di una dimensione prefissata del documento – oppure in forma testuale, usando il viewer di testo integrato – al di sopra di tale soglia – in funzione della dimensione del documento, poiché Internet Explorer, che offre una visualizzazione ad albero particolarmente piacevole, presenta problemi di efficienza con documenti di grandi dimensioni. La soglia effettiva è configurabile dall'utente.

4.9.5 Il *plug-in* "Firma e Cifra" per il formato .p7e

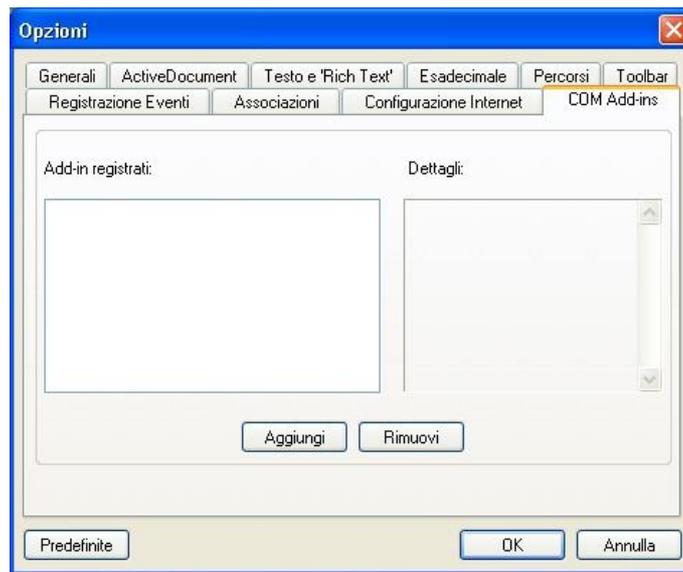
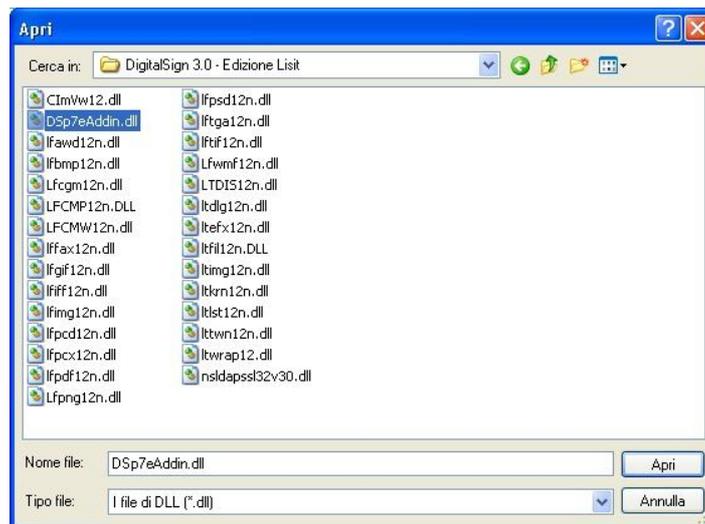
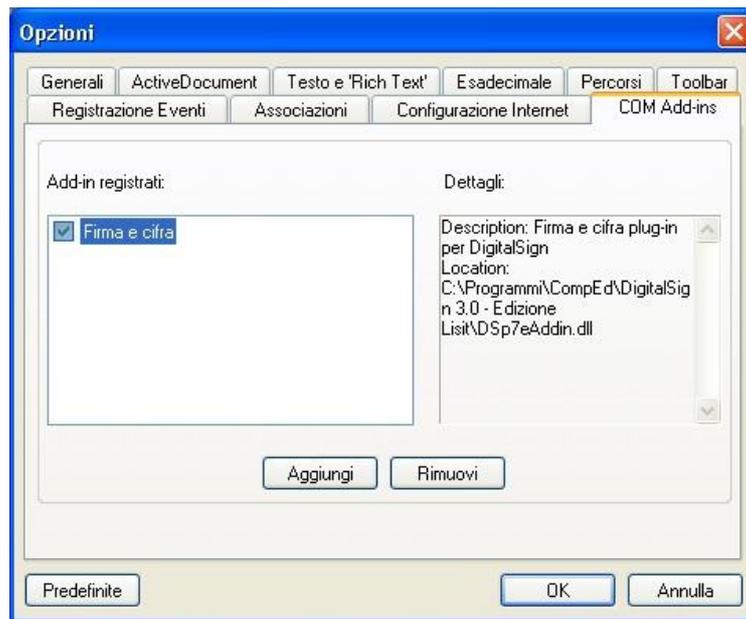
Quantunque DigitalSign sia in grado di combinare, in una singola struttura PKCS#7, sia la firma digitale che la crittografia dei contenuti, alcuni altri prodotti software adottano una tecnica

differente basata su due diverse “envelope” PKCS#7: la più interna contiene il documento con la firma digitale; tale struttura viene poi considerata come il “contenuto” di un ulteriore documento PKCS#7, più esterno, che viene cifrato.

DigitalSign è comunque in grado di aprire un documento di questo tipo, evidenziando la struttura a doppia envelope:

Questa stessa struttura si può riprodurre manualmente, con DigitalSign, procedendo prima con l’apposizione della firma digitale, quindi riaprendo il documento come *contenuto di un nuovo documento* ed infine operando la cifratura.
Naturalmente questo procedimento è un po’ macchinoso; è quindi stato predisposto un “plug-in” utile proprio nel caso rivoglia produrre un documento destinato ad essere aperto con prodotti non in grado di gestire firma digitale e cifratura nella stessa *envelope* PKCS#7.

4.9.5.1 Installazione del plug-in

Alcune edizioni di DigitalSign contengono già il plug-in all’origine e non richiedono quindi alcuna installazione.
Qualora non sia questo il nostro caso, il plug-in consiste di una DLL memorizzata nel sistema (preferibilmente nella stessa cartella che ospita l’eseguibile di DigitalSign).

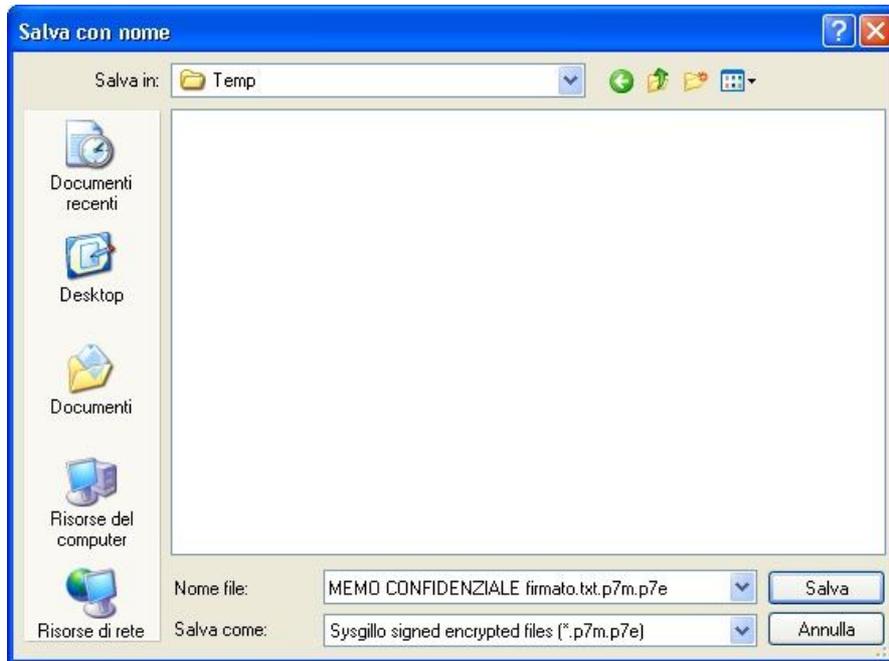
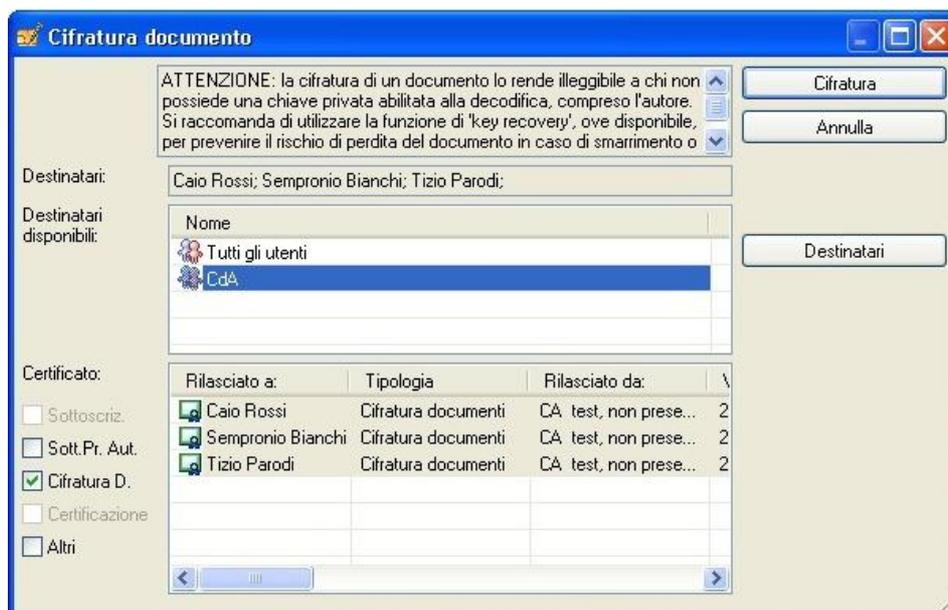
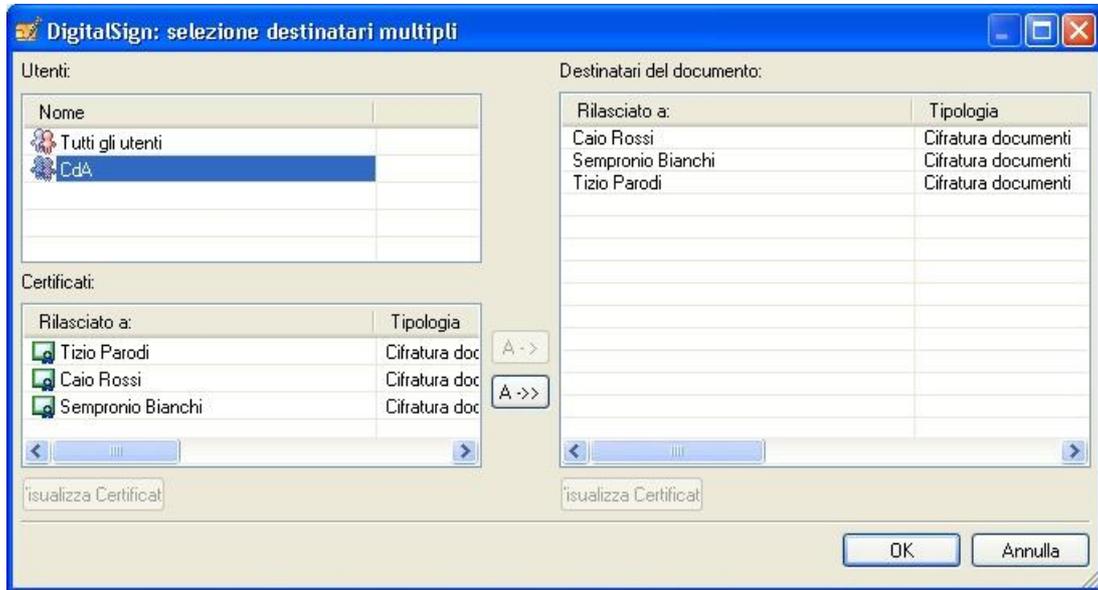
Si opera dal menu **Strumenti -> Opzioni ->** tab **COM Add-Ins**. Immaginando di non avere ancora installato alcun plug-in si vedrà questa finestra:

Si aziona il bottone Aggiungi e si seleziona il file che costituisce il plug-in (DSp7eAddin.dll):

La finestra degli add-in si aggiornerà come segue:

Alla chiusura del pannello delle Opzioni DigitalSign verrà reinizializzato, quindi dovrà comparire il nuovo bottone nella toolbar:

Il menu Strumenti viene arricchito di una nuova voce specifica del plug-in, che a sua volta contiene un sottomenu limitato ad una sola opzione:

4.9.5.2 Utilizzo del plug-in

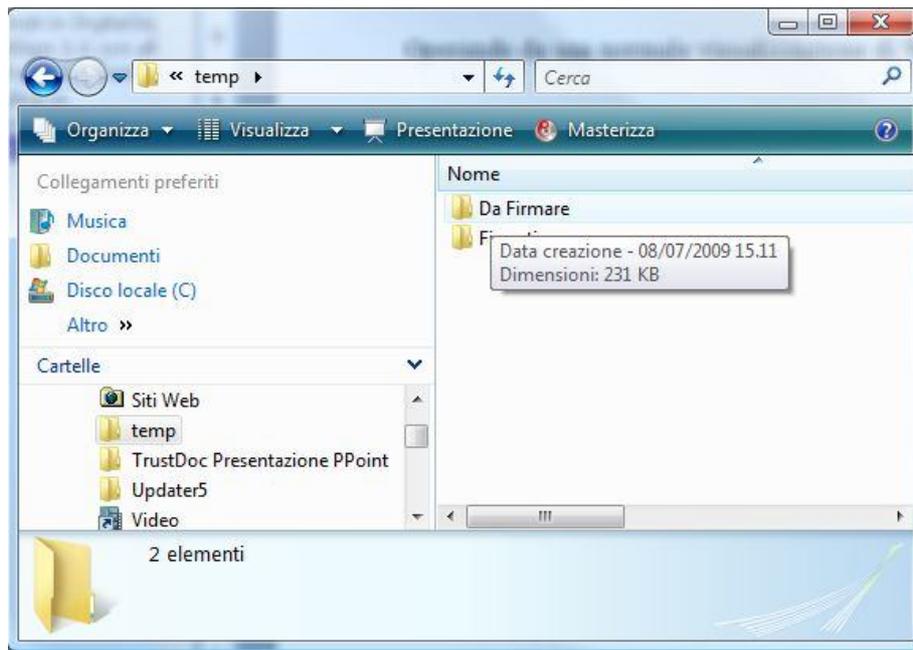
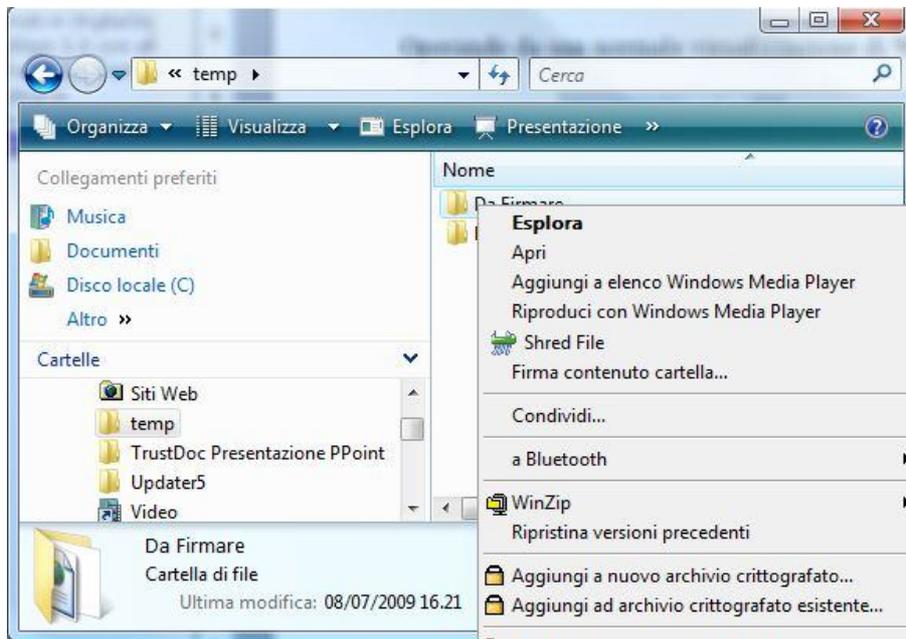
Si noti che il plug-in, avendo come obiettivo la produzione di documenti firmati e cifrati in doppia *envelope* PKCS#7, richiede di essere attivato a partire da un documento già firmato.

Quindi occorre predisporre un documento di tali caratteristiche (aprendolo da un file .p7m oppure costruendolo con le normali funzioni di DigitalSign) ed infine attivare il plug-in per mezzo della funzione del menu **Strumenti -> Firma e Cifra -> Salva come file *.p7m.p7e**

Apparirà una consueta finestra di selezione del nome del file per il salvataggio, con il nome definitivo già formato in modo corretto e con il tipo "p7e" già impostato:

Una volta confermato il nome del file vengono presentate la consuete finestre per la selezione del destinatario o dei destinatari per la cifratura (si veda la sezione dedicata):

Anche in questo contesto, con **Cifratura** si completa il processo (dopo aver selezionato un certificato), oppure con **Destinatari** si passa ad una ulteriore finestra per la sezione di destinatari multipli:

Si noti che ricorrendo a questa seconda finestra ausiliaria, agendo su OK si chiude la finestra ma si torna alla precedente, che si chiude con **Cifratura** per completare il processo.

4.9.6 Firma semiautomatica dalla *shell* di Windows

Se a livello di Opzioni -> Associazioni viene opportunamente abilitata l'opzione **Tutti gli altri tipi** (si veda la sezione relativa), DigitalSign offrirà dalla *shell* di Windows la possibilità di attivare direttamente la firma semiautomatica di tutti i documenti presenti in una data cartella senza passare per la normale interfaccia di DigitalSign.

Operando da una normale visualizzazione di Windows Explorer, si localizzi la cartella su cui agire:

Quindi, facendo click con il tasto destro del mouse sulla cartella (nel nostro caso Da Firmare) si vedrà un menu proprio di Windows. Il contenuto effettivo del nostro menu dipende dalle applicazioni che abbiamo installato:

A noi adesso interessa la voce **Firma contenuto cartella**: agendo su questa opzione si lancerà DigitalSign (se non è già attivo) e si passa automaticamente alla condizione corrispondente alla voce del menu **File -> Firma contenuto cartella**, cui è dedicata una sezione di questa guida.